UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

ATLAS DATA PRIVACY CORPORATION, *as assignee of individuals who are Covered Persons*, JANE DOE-1, *a law enforcement officer*, JANE DOE-2, *a law enforcement officer*, PATRICK COLLIGAN, and PETER ANDREYEV, Plaintiffs, v. GREENFLIGHT VENTURE CORP., RICHARD ROES 1-10, *fictitious names of unknown individuals* and ABC COMPANIES 1-10, *fictitious names of unknown entities*, Defendants.	**Case No.: 25-cv-1517-HB** **CIVIL ACTION** **DEFENDANT GREENFLIGHT VENTURE CORP.'S MOTION TO DISMISS PLAINTIFFS' COMPLAINT, PURSUANT TO FED. R. CIV. P. 12(b)(6)** Motion Returnable: April 22, 2025 Oral Argument is Requested

PLEASE TAKE NOTICE that, on April 22, 2025, or as soon thereafter as counsel may be heard, pursuant to that which was discussed during a status conference on or about March 4, 2025, Defendant Greenflight Venture Corp., without prejudice to other potential motions and without waiving any of its rights, shall move before the Honorable Harvey Bartle, III, U.S.D.J., at the United States District Court for the District of New Jersey, Mitchell H. Cohen Building & U.S. Courthouse, 4th & Cooper Streets, Camden, New Jersey 08101, for an Order dismissing Plaintiffs' Complaint in its entirety, with prejudice, pursuant to Fed. R. Civ. P. 12(b)(6).

PLEASE TAKE FURTHER NOTICE, that in support of this Motion to Dismiss, Defendant Greenflight Venture Corp., incorporates fully herein the Memorandum of Law filed by various other Defendants in related actions in what is referred to in those actions as the Consolidated Motion to

Dismiss, filed in this Court on June 10, 2024, under Docket No.: 1:24-cv-04105, which is annexed hereto as **Exhibit A**. For the Court's convenience, Defendant Greenflight Venture Corp. also submits the foregoing Supplement to the Motion to Dismiss for purposes of the record before this Court, to address facts uniquely applicable to Defendant's position regarding OKCaller.

Respectfully submitted,
Law Offices of Jared M. Wichnovitz, P.C.
Attorneys for Defendant, Greenflight Venture Corp.

/s/ *Jared M. Wichnovitz*

JARED M. WICHNOVITZ, ESQ.
Bar I.D. 414022022
Law Offices of Jared M. Wichnovitz, P.C.
50 Harrison Street, Suite 206
P.O. Box 631
Hoboken, New Jersey 07030
Office: (732) 765-2157
Fax: (732) 358-0178
Email: Jared@WichnovitzLaw.com

SUPPLEMENTAL MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

I. INTRODUCTION

OkCaller was founded in 2014 to enhance telephone safety on the internet. For decades prior, caller ID remained under the purview of large telecom companies, and many cell phones either lacked caller ID altogether or provided it only at prohibitive cost. Text-message caller ID was essentially unavailable. This absence of widespread, affordable caller-identification features led to serious safety issues—such as phishing attacks, spam/harassing texts, and calls to cell phones that failed to identify the sender or caller.

OkCaller changed that dynamic. Through its patented "web caller ID bridge," OkCaller provides free reverse-lookup caller-name identification online. To date, it has furnished free caller ID services to nearly 300 million users, in full transparency and without resorting to data broker practices. This proprietary system is covered by a U.S. Reissue Patent invented by Dr. Jeffrey Isaacs of Fort Washington, Pennsylvania.

As classified by the U.S. Patent and Trademark Office, OkCaller operates as a *telephonic communication directory utility*. From its inception in 2014, OkCaller has strived to implement caller ID responsibly so that crucial safety benefits are available to everyone. OkCaller's Terms of Service define that users engage OkCaller as their *telephone services provider* for the limited purpose of obtaining caller ID functionality. Moreover, those Terms prohibit "forward searches" and only allow a user to perform a reverse lookup if they already have the caller's telephone number via an incoming call or text. At that point, OkCaller supplies a name and *nothing more*.

Hence, OkCaller is fully compliant with Daniel's Law and exempt as a telephone directory since it never provides unpublished phone numbers or addresses of covered persons. Notwithstanding its compliance, OkCaller promptly suspended service for all New Jersey area codes upon receiving Atlas's sweeping claims—pending the outcome of this motion and litigation. This enforced

interruption jeopardizes vital public-safety features of caller ID, contrary to Atlas's unfounded assertions. Accordingly, Defendants respectfully request a prompt and timely resolution of these issues. As set forth below, there are profound constitutional concerns with Atlas's expansive framing of Daniel's Law that threaten OkCaller's lawful and important telephonic directory service.

Unlike the data brokers or large internet services at issue in most *Daniel's Law* litigation, OkCaller does not store or publicly display private or unpublished addresses or phone numbers. Instead, users who have received an incoming call or text voluntarily input the calling number into OkCaller's patented system—disclosing nothing about the person's private address—and merely receive the caller's name back. This reverse lookup function fills an important public safety need by helping people discern who has contacted them, thereby reducing spam, fraud, and harassment.

Despite these limited, lawful, and safety-enhancing activities, Plaintiffs attempt to sweep OkCaller into liability under *Daniel's Law* (N.J.S.A. 56:8-166.1, et seq.) for allegedly disclosing "personal identifiable information" about covered persons. These claims are constitutionally untenable and factually baseless. As explained below (and in the Consolidated Motion, incorporated herein), the application of *Daniel's Law* to OkCaller violates the First Amendment under multiple doctrines, is impermissibly vague, and disregards OkCaller's plain exemption as a "telephone directory" or "telephonic network directory utility" that does not disclose addresses or "unpublished telephone numbers."

Due to these meritless claims, OkCaller's critical service has already been suspended for New Jersey area codes, causing actual harm to consumers who rely on OkCaller for safety—due to these meritless claims. OkCaller respectfully requests prompt dismissal of all claims against it, consistent with the constitutional and statutory arguments raised by the other Defendants and as applied here with even greater force, given OkCaller's distinctive function and compliance posture.

II. BACKGROUND

Founded in 2014 by Dr. Jeffrey Isaacs (Fort Washington, PA), OkCaller pioneered free "web-based caller ID," bridging the gap between costly legacy telecom caller ID services and consumer demand for incoming-text and -call identification. Through U.S. Reissue Patent No. RE48,847 (**EXHIBIT B)**, OkCaller's authorized technology allows a user—who already has a 10-digit incoming phone number—to receive the name of the calling or texting party. Importantly, OkCaller does not provide addresses, nor does it disclose any phone number the consumer did not already have.

OkCaller's Terms of Service (hereinafter "TOS") prohibit "forward searches" (i.e., searching for a person's phone number by name). Instead, callers must already possess the calling party's phone number from an incoming call or text and may only request the "calling party name." No addresses or unpublished phone numbers are ever displayed or provided. OkCaller's TOS also explains that individuals can "opt out" of being identified by name via either (a) calling their phone carrier to block CNAM (Caller Name) or (b) OkCaller's own SMS-based opt-out procedure.

B. Atlas's Claims

Atlas contends that *Daniel's Law* (as amended) prohibits any disclosure or "making available" of covered persons' personal information upon receipt of a takedown notice, and it seeks to impose "liquidated damages" for alleged violations. In the *Consolidated Motion to Dismiss*, the numerous Defendants set forth significant constitutional challenges to *Daniel's Law*'s overbreadth, content-based restrictions, lack of narrow tailoring, and impermissible vagueness. All these arguments apply with enhanced force to OkCaller, given that OkCaller (unlike many other Defendants) discloses no addresses or unpublished phone numbers and is, by definition, a "telephone directory" providing only published CNAM data for legitimate caller-identification needs.

III. ARGUMENT

Defendant fully joins and adopts by reference the arguments set forth in the *Consolidated Motion to Dismiss*. However, OkCaller's circumstances exemplify the overbreadth and vagueness of *Daniel's Law* even more starkly. Indeed, the law's forced application to OkCaller leads to absurd and unconstitutional results – that a telephone company cannot communicate with its customers about "covered persons." This is a clear First Amendment violation, by any definition.

A. Daniel's Law Imposes a Content-Based Restriction That Fails Strict Scrutiny, Particularly as Applied to OkCaller's Caller ID Service

As discussed in the Consolidated Motion, *Daniel's Law* is a content-based speech restriction because it singles out the communication of certain information (home address or unpublished phone number) and restricts it based on its content. (*See* Consol. Mot.) Generally, although OkCaller does not disclose addresses or unpublished phone numbers, Atlas's sweeping theory suggests even revealing a name (at the user's voluntary request) or a telephone user *conveying a telephone number they already know* might violate *Daniel's Law* if the underlying phone number belongs to a "covered person."

1. No Legitimate State Interest Served by Prohibiting Caller ID

Even if the Court assumes *Daniel's Law* is intended to protect public officials, the forced extension of the statute to bar legitimate caller-identification services does not serve that interest. Indeed, OkCaller's function enhances public safety. Telling a consumer "You received a call from *John Doe*, not an unknown spammer" does not harm or endanger a covered person; it prevents anonymous harassment by enabling the callee to see who is calling. (*See* Consol. Mot. discussing over- and under-inclusiveness.)

2. **Strikingly Overinclusive as Applied to OkCaller**

While *Daniel's Law* purports to stop the harmful disclosure of addresses or phone numbers, it in no way contemplates shutting down essential telephone directory utilities that do not publicly post those addresses. Yet Atlas insists on a reading that penalizes OkCaller for purely private, user-initiated requests about phone numbers they already possess. That vast overreach belies the notion of narrow tailoring.

3. **Underinclusive for Actual Harms While Overburdening Harmless Speech**

Simultaneously, *Daniel's Law* fails to prohibit myriad sources of true "home address" publication, including county or municipal websites, property records, or self-publication by the covered person. Yet it threatens OkCaller with liability for simply providing CNAM to an existing phone number—an almost perfect "reverse search" scenario that reveals no address and possess zero risk. This underinclusive/overinclusive mismatch contravenes the Supreme Court's requirement that content-based laws use the "least restrictive means." (*See* Consol. Mot. Discussion of *McCullen v. Coakley*, 573 U.S. 464, 494 (2014).)

B. Even If Deemed Content-Neutral, Daniel's Law Fails Intermediate Scrutiny Given Its Application to OkCaller

The Consolidated Motion further shows that even under an alternative, lower standard (i.e., *Central Hudson* or intermediate scrutiny), *Daniel's Law* still fails because it does not directly advance its stated aim and burdens far more speech than necessary. As to OkCaller, the alleged "interest" is preventing disclosure of protected individuals' addresses or unpublished numbers. OkCaller never provides such information.OkCaller's output is simply the caller's name—lawfully obtained from

legitimate CNAM data. There is thus no "reasonable fit" between banning OkCaller's reverse-lookup feature and protecting a covered person's private address or unlisted phone number.

Nothing in *Daniel's Law* or legislative history suggests the intention to halt telephone directory services. Yet Atlas's claims seek precisely that outcome—an unconstitutional burden on free expression and free association without advancing any genuine public-safety interest.

C. The Statute Is Unconstitutionally Vague as Applied to OkCaller

OkCaller's experience highlights the confusion surrounding *Daniel's Law*'s sweeping definitions of "disclose or otherwise make available." (N.J.S.A. 56:8-166.1(a)(1).) The phrase could ostensibly capture any transmission or partial mention of a phone number. As OkCaller's system operates only when a user (callee) enters a phone number they already have, it is unclear how or why OkCaller would be roped into liability for "disclosure" of addresses or unpublished phone numbers. Further, *Daniel's Law* specifically addresses "home address" and "unpublished home telephone number." (N.J.S.A. 56:8-166.1(a)(1).) Yet Atlas's suit erroneously conflates that with the public CNAM data OkCaller retrieves. Imposing large statutory damages on OkCaller for "violations" that do not implicate *Daniel's Law* fosters exactly the unconstitutional vagueness the Consolidated Motion describes. (*See* Consol. Mot. citing *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253–54 (2012).)

D. OkCaller's Suspension of Service Illustrates the Chilling Effect

As an immediate response to Atlas's claims, OkCaller stopped providing caller ID functionality to all New Jersey area codes to avoid the risk of crushing "liquidated damages." This self-censorship underscores the profound chilling effect a vague or overbroad application of Daniel's Law creates, harming the very users the law purports to protect by denying them essential and lawful caller-ID safety services.

IV. OKCALLER IS UNIQUELY POSITIONED FOR DISMISSAL

Although the consolidated arguments demonstrate that *Daniel's Law* (as interpreted by Atlas) is facially unconstitutional, it is especially misguided as applied to OkCaller. OkCaller's patented process for identifying who called a user—based on the user's already-known 10-digit number—mirrors a standard telephone-directory function. By legislative design, directories (and specifically published telephone numbers) have historically been exempt from many "do not disclose" prohibitions. Atlas's own allegations nowhere identify any instance of OkCaller providing a home address or an unpublished phone number and thus fail to state a claim for various other reasons, Defendants reserve all rights to raise. OkCaller's TOS categorically bars forward searches or mass access to PII.

Daniel's Law aims to reduce threats against public officials yet stopping OkCaller's caller ID fosters anonymous phone-based harassment. The application of the statute to bar OkCaller's safe, narrow function inverts the law's intent.

Safety of Opt-Outs and the Impracticality of Atlas's Approach

OkCaller's caller ID opt-out mechanisms—and telephone carriers' decades-old protocols—have protected privacy for nearly fifty years without creating any documented safety incident. Under existing industry practice**,** the Primary Carrier Is the Opt-Out Point. Most phone subscribers manage their "Caller ID Name" (CNAM) settings—such as specifying a spouse's or child's name, or opting out entirely—directly through the account portal provided by major carriers (Verizon, AT&T, T-Mobile). Once a subscriber disables or blocks their outgoing caller ID with the carrier, OkCaller and all other lawful "syndicates" of CNAM data automatically receive that opt-out through the standard LIDB GR-1188 telecom protocol.

For further assurance, OkCaller allows users to text a PIN from the number they wish to remove, verifying ownership and identity. Upon successful completion, OkCaller's system instantly ceases to return that name in any caller-ID lookup. Notably, OkCaller does not even "maintain" the data subject to Daniel's law – its website plainly discloses that it acts as a real-time telephone utility connection, relaying CNAM data via GR-1188 to the customer.

These two parallel methods have *collectively functioned for half a century* without incident or exploitation. Atlas, however, seeks to insert itself into this well-established system as a "middleman" without employing PIN verification or verifying that the requestor truly owns the relevant phone number. Indeed, Atlas's approach—inviting "email-only" opt-outs—risks creating new security vulnerabilities, allowing *anyone* to take down, or worse, *modify*, legitimate caller IDs improperly. Does Atlas verify phone company ownership of a number before sending its requests, or notary public confirmation of identification documents? This is precisely why OkCaller's Terms explicitly prohibit unauthorized "mass third-party" takedowns of its caller ID system.

Crucially, Daniel's Law was not designed to enable third parties to disrupt legitimate telephone directory utilities or impose an unverified, email-based takeover of existing CNAM processes. Atlas's interpretation effectively subverts the very safety interests Daniel's Law purportedly protects—by injecting confusion and potential abuse into a proven telecom framework.

For these reasons, immediate judicial clarification is vital. The Court should either rule that telephone directory providers like OkCaller are exempt from Daniel's Law (consistent with both the letter and spirit of the statute) or find the law unconstitutional *as applied*, for the reasons detailed in Defendants' Consolidated Motion to Dismiss, which OkCaller fully adopts and concurs with here. Absent such a ruling, OkCaller's indisputably legitimate caller-ID operations will remain chilled, depriving consumers of an essential safety service and upending half a century of successful, stable carrier-based opt-out solutions.

V. CONCLUSION

OkCaller's free reverse-lookup service is precisely the kind of minimal, lawful consumer telephone directory function that—far from violating the letter or spirit of *Daniel's Law*—helps safeguard the public from anonymous, harmful communications. Applying *Daniel's Law* to OkCaller's essential service would violate the First Amendment, result in impermissible vagueness, and produce undesireable real-world consequences that contravene both the statute's stated purpose and common sense.

For the foregoing reasons, as well as those set forth in the Consolidated Motion to Dismiss, Defendant respectfully requests that this Court dismiss with prejudice all claims against it, declare that OkCaller may exercise the patent awarded to it by USPTO, and award such further relief as this Court deems appropriate.

Dated: March 17, 2025

Respectfully submitted,
Law Offices of Jared M. Wichnovitz, P.C.
Attorneys for Defendant, Greenflight Venture Corp.

/s/ *Jared M. Wichnovitz*

JARED M. WICHNOVITZ, ESQ.
Bar I.D. 414022022
Law Offices of Jared M. Wichnovitz, P.C.
50 Harrison Street, Suite 206
P.O. Box 631
Hoboken, New Jersey 07030
Office: (732) 765-2157
Fax: (732) 358-0178
Email: Jared@WichnovitzLaw.com

CERTIFICATE OF SERVICE

I hereby certify that on March 17, 2025, a true and correct copy of the foregoing Motion to Dismiss with all exhibits was served via ECF Filing on PACER upon:

Counsel for Plaintiffs:

Rajiv D. Parikh, Esq.

Dated: March 17, 2025

Law Offices of Jared M. Wichnovitz, P.C.
Attorneys for Defendant, Greenflight Venture Corp.

/s/ *Jared M. Wichnovitz*
JARED M. WICHNOVITZ, ESQ.

EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

ATLAS DATA PRIVACY CORPORATION, et al. v. BLACKBAUD, INC., et al.	CIVIL ACTION NO. 24-3993 (Hon. Harvey Bartle, III) **Oral Argument Requested** **Motion Day: September 3, 2024**
ATLAS DATA PRIVACY CORPORATION, et al. v. WHITEPAGES, INC., et al.	CIVIL ACTION NO. 24-3998
ATLAS DATA PRIVACY CORPORATION, et al. v. HIYA, INC., et al.	CIVIL ACTION NO. 24-4000
ATLAS DATA PRIVACY CORPORATION, et al. v. WE INFORM, LLC, et al.	CIVIL ACTION NO. 24-4037
ATLAS DATA PRIVACY CORPORATION, et al. v. INFOMATICS, LLC, et al	CIVIL ACTION NO. 24-4041
ATLAS DATA PRIVACY CORPORATION, et al. v. THE PEOPLE SEARCHERS, LLC, et al.	CIVIL ACTION NO. 24-4045

ATLAS DATA PRIVACY CORPORATION, et al. v. COMMERCIAL REAL ESTATE EXCHANGE, INC., et al.	CIVIL ACTION NO. 24-4073
ATLAS DATA PRIVACY CORPORATION, et al. v. DM GROUP, INC., et al.	CIVIL ACTION NO. 24-4075
ATLAS DATA PRIVACY CORPORATION, et al. v. CARCO GROUP INC., et al.	CIVIL ACTION NO. 24-4077
ATLAS DATA PRIVACY CORPORATION, et al. v. DELUXE CORPORATION, et al.	CIVIL ACTION NO. 24-4080
ATLAS DATA PRIVACY CORPORATION, et al. v. TWILIO INC., et al.	CIVIL ACTION NO. 24-4095
ATLAS DATA PRIVACY CORPORATION, et al. v. QUANTARIUM ALLIANCE, LLC, et al.	CIVIL ACTION NO. 24-4098
ATLAS DATA PRIVACY CORPORATION, et al. v. YARDI SYSTEMS, INC., et al.	CIVIL ACTION NO. 24-4103

ATLAS DATA PRIVACY CORPORATION, et al. v 6SENSE INSIGHTS, INC., et al.	CIVIL ACTION NO. 24-4104
ATLAS DATA PRIVACY CORPORATION, et al. v. LIGHTBOX PARENT, L.P., et al.	CIVIL ACTION NO. 24-4105
ATLAS DATA PRIVACY CORPORATION, et al. v. SEARCH QUARRY, LLC, et al.	CIVIL ACTION NO. 24-4106
ATLAS DATA PRIVACY CORPORATION, et al. v. ACXIOM, LLC, et al.	CIVIL ACTION NO. 24-4107
ATLAS DATA PRIVACY CORPORATION, et al. v. ENFORMION, LLC, et al.	CIVIL ACTION NO. 24-4110
ATLAS DATA PRIVACY CORPORATION, et al. v. COSTAR GROUP, INC., et al.	CIVIL ACTION NO. 24-4111
ATLAS DATA PRIVACY CORPORATION, et al. v. ORACLE INTERNATIONAL CORPORATION, et al.	CIVIL ACTION NO. 24-4112

ATLAS DATA PRIVACY CORPORATION, et al. v. RED VIOLET, INC., et al.	CIVIL ACTION NO. 24-4113
ATLAS DATA PRIVACY CORPORATION, et al. v. RE/MAX, LLC, et al.	CIVIL ACTION NO. 24-4114
ATLAS DATA PRIVACY CORPORATION, et al. v. EPSILON DATA MANAGEMENT, LLC, et al.	CIVIL ACTION NO. 24-4168
ATLAS DATA PRIVACY CORPORATION, et al. v. PEOPLE DATA LABS, INC., et al.	CIVIL ACTION NO. 24-4171
ATLAS DATA PRIVACY CORPORATION, et al. v. LABELS & LISTS, INC., et al.	CIVIL ACTION NO. 24-4174
ATLAS DATA PRIVACY CORPORATION, et al. v. CLARITAS, LLC, et al.	CIVIL ACTION NO. 24-4175
ATLAS DATA PRIVACY CORPORATION, et al. v. INNOVIS DATA SOLUTIONS INC., et al.	CIVIL ACTION NO. 24-4176

ATLAS DATA PRIVACY CORPORATION, et al. v. ACCURATE APPEND, INC., et al.	CIVIL ACTION NO. 24-4178
ATLAS DATA PRIVACY CORPORATION, et al. v. DATA AXLE, INC., et al.	CIVIL ACTION NO. 24-4181
ATLAS DATA PRIVACY CORPORATION, et al. v. REMINE INC., et al.	CIVIL ACTION NO. 24-4182
ATLAS DATA PRIVACY CORPORATION, et al. v. LUSHA SYSTEMS, INC., et al.	CIVIL ACTION NO. 24-4184
ATLAS DATA PRIVACY CORPORATION, et al. v. TELTECH SYSTEMS, INC., et al.	CIVIL ACTION NO. 24-4217
ATLAS DATA PRIVACY CORPORATION, et al. v. PEOPLECONNECT, INC., et al.	CIVIL ACTION NO. 24-4227
ATLAS DATA PRIVACY CORPORATION, et al. v. CORELOGIC, INC., et al.	CIVIL ACTION NO. 24-4230

ATLAS DATA PRIVACY CORPORATION, et al. v. BLACK KNIGHT TECHNOLOGIES, LLC, et al.	CIVIL ACTION NO. 24-4233
ATLAS DATA PRIVACY CORPORATION, et al. v. ZILLOW, INC., et al.	CIVIL ACTION NO. 24-4256
ATLAS DATA PRIVACY CORPORATION, et al. v. EQUIMINE, INC., et al.	CIVIL ACTION NO. 24-4261
ATLAS DATA PRIVACY CORPORATION, et al. v. THOMSON REUTERS CORPORATION, et al.	CIVIL ACTION NO. 24-4269
ATLAS DATA PRIVACY CORPORATION, et al v. CHOREOGRAPH LLC, et al.	CIVIL ACTION NO. 24-4271
ATLAS DATA PRIVACY CORPORATION, et al. v. TRANSUNION, LLC, et al	CIVIL ACTION NO. 24-4288

ATLAS DATA PRIVACY CORPORATION, et al. v. MELISSA DATA CORP., et al.	CIVIL ACTION NO. 24-4292
ATLAS DATA PRIVACY CORPORATION, et al. v. EQUIFAX INC., et al.	CIVIL ACTION NO. 24-4298
ATLAS DATA PRIVACY CORPORATION, et al. v. SPOKEO, INC., et al.	CIVIL ACTION NO. 24-4299
ATLAS DATA PRIVACY CORPORATION, et al. v. i360, LLC, et al.	CIVIL ACTION NO. 24-4345
ATLAS DATA PRIVACY CORPORATION, et al. v. TELNYX LLC, et al.	CIVIL ACTION NO. 24-4354
ATLAS DATA PRIVACY CORPORATION, et al. v. GOHUNT, LLC, et al.	CIVIL ACTION NO. 24-4380
ATLAS DATA PRIVACY CORPORATION, et al. v. ACCUZIP, INC., et al.	CIVIL ACTION NO. 24-4383

ATLAS DATA PRIVACY CORPORATION, et al. v. SYNAPTIX TECHNOLOGY, LLC, et al.	CIVIL ACTION NO. 24-4385
ATLAS DATA PRIVACY CORPORATION, et al. v. JOY ROCKWELL ENTERPRISES, INC., et al.	CIVIL ACTION NO. 24-4389
ATLAS DATA PRIVACY CORPORATION, et al. v. FORTNOFF FINANCIAL, LLC, et al.	CIVIL ACTION NO. 24-4390
ATLAS DATA PRIVACY CORPORATION, et al. v. MYHERITAGE, LTD., et al.	CIVIL ACTION NO. 24-4392
ATLAS DATA PRIVACY CORPORATION, et al. v. E-MERGES.COM, INC., et al.	CIVIL ACTION NO. 24-4434
ATLAS DATA PRIVACY CORPORATION, et al. v. WILAND, INC., et al.	CIVIL ACTION NO. 24-4442
ATLAS DATA PRIVACY CORPORATION, et al. v. ATDATA, LLC, et al.	CIVIL ACTION NO. 24-4447

ATLAS DATA PRIVACY CORPORATION, et al. v. PRECISELY HOLDINGS, LLC, et al.	CIVIL ACTION NO. 24-4571
ATLAS DATA PRIVACY CORPORATION, et al. v. NUWBER, INC., et al.	CIVIL ACTION NO. 24-4609
ATLAS DATA PRIVACY CORPORATION, et al. v. ROCKETREACH LLC, et al.	CIVIL ACTION NO. 24-4664
ATLAS DATA PRIVACY CORPORATION, et al. v. OUTSIDE INTERACTIVE INC., et al.	CIVIL ACTION NO. 24-4696
ATLAS DATA PRIVACY CORPORATION, et al. v. VALASSIS DIGITAL CORP., et al.	CIVIL ACTION NO. 24-4770
ATLAS DATA PRIVACY CORPORATION, et al. v. THE LIFETIME VALUE CO. LLC, et al.	CIVIL ACTION NO. 24-4850
ATLAS DATA PRIVACY CORPORATION, et al. v. BELLES CAMP COMMUNICATIONS, INC., et al.	CIVIL ACTION NO. 24-4949

ATLAS DATA PRIVACY CORPORATION, et al. v. FIRST AMERICAN FINANCIAL CORPORATION., et al.	CIVIL ACTION NO. 24-5334
ATLAS DATA PRIVACY CORPORATION, et al. v. PROPERTY RADAR INC., et al.	CIVIL ACTION NO. 24-5600
ATLAS DATA PRIVACY CORPORATION, et al. v. THE ALESCO GROUP, L.L.C., et al.	CIVIL ACTION NO. 24-5656
ATLAS DATA PRIVACY CORPORATION, et al. v. SEARCHBUG, INC., et al.	CIVIL ACTION NO. 24-5658
ATLAS DATA PRIVACY CORPORATION, et al. v. AMERILIST, INC. et al.	CIVIL ACTION NO. 24-5775
ATLAS DATA PRIVACY CORPORATION, et al. v. LEXISNEXIS RISK DATA MANAGEMENT, LLC, et al.	CIVIL ACTION NO. 24-6160

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' CONSOLIDATED MOTION TO DISMISS PLAINTIFFS' COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

I. INTRODUCTION

Daniel's Law started as a laudable effort by the State of New Jersey to enhance the safety of judges, law enforcement, and other public officials, but the statute in its current form—particularly as most recently amended through lobbying efforts by Plaintiffs' counsel—is not appropriately tailored to this end. The statute provides that, upon receipt of a notification provided by a covered person, "any person or business association" shall not "disclose" or "otherwise make available" the covered person's home address or phone number. But the statute's sweeping definition of "disclose" encompasses *any* transfer of this information of any kind, including transfers between businesses, or even within *the same* business; and the catchall phrase "otherwise make available" makes the statute even *more* open-ended and hopelessly vague. On top of this, the statute imposes "liquidated damages" triggered by a short and arbitrary compliance deadline, without any consideration of fault or extenuating circumstances. At the same time, the statute contains broad-reaching exceptions—most significantly for disclosure of records by public agencies—that undermine the very purpose the statute was intended to serve. For all these reasons, the statute is facially unconstitutional under the First Amendment and the New Jersey Free Speech Clause.

Contrary to Plaintiffs' assertions, Defendants do not bring this challenge because they seek to profit at the expense of the safety of public officials. It is instead

the lead Plaintiff, Atlas Data Privacy, that is pursuing profit here instead of seeking to protect anyone's safety. Having lobbied the legislature for a bespoke assignment provision, Atlas and its counsel launched this litigation project by cynically abusing that provision. They recruited over 19,000 alleged covered persons to purportedly assign their Daniel's Law claims to Atlas through a mass-marketing campaign, took no action for *months* while this recruitment effort was conducted (belying any concern for the safety of the "assignors"), and then bombarded well over a hundred companies with thousands of takedown requests over a short period of time, including over the year-end holidays, in an attempt to frustrate the companies' ability to comply within the ostensible statutory deadline—all to gin up claims for "liquidated damages." Notably, many unsuspecting defendants named in these cases are small businesses, some of which cannot afford to defend these cases, let alone survive the astronomical damages Atlas indiscriminately seeks.

Atlas's misuse of Daniel's Law only highlights the statute's excessive breadth—making it *susceptible* to abuse—and the corresponding justification for invalidating the statute under the First Amendment. The statute imposes content-based restrictions on protected speech and is thus subject to strict scrutiny—which the statute cannot survive because it is not narrowly tailored to the state interest it is supposed to serve. Even if analyzed under an intermediate-scrutiny standard, Daniel's Law would fail, because it is not even *reasonably* tailored to the state's

interest. The statute is also unconstitutionally vague, because it does not provide sufficient notice of what it prohibits and invites arbitrary enforcement. Accordingly, the statute should be invalidated, and this litigation dismissed, with prejudice.

II. BACKGROUND

A. Daniel's Law

1. The Statute Imposes Sweeping Prohibitions, Rigid Deadlines, and Harsh Penalties on Private Businesses

In July 2020, United States District Judge Esther Salas's only son, Daniel Anderl, was murdered at Judge Salas's home by a disgruntled lawyer who had litigated before her. Compl. ¶ 5.[1] In response to that unspeakable tragedy, the New Jersey State Legislature enacted Daniel's Law, P.L. 2020, c. 125 (codified at N.J.S.A. 47:1A-1–A-3 and N.J.S.A. 56:8-166.1), aimed at protecting the safety of certain government officials. Compl. ¶ 8.

The civil provisions of Daniel's Law provide that, upon "notification" made by a "covered person"—defined to include active and retired judges, law enforcement officers, and certain other public officials, as well as any immediate family member residing in the same household—a "person, business or association"

---

[1] All docket citations are to the Complaint filed against Defendant Blackbaud, Inc., et al. (hereafter, "Compl."), Ex. 1, and to the docket in *Atlas Data Privacy Corp. et al v. Blackbaud Inc., et al*, No. 1:24-cv-03993-HB (D.N.J). All other Complaints filed by Atlas are materially the same. All citations to exhibits are to those attached to the Declaration of Serrin Turner, submitted herewith.

shall not "disclose or re-disclose or otherwise make available" the covered person's "home address or unpublished home telephone number." N.J.S.A. 56:8-166.1(a)(1), (d). The statute does not specify how such a non-disclosure "notification" is to be made, other than stating that it must be a "written notice . . . requesting that the person [to whom the notice is directed] cease the disclosure of [the covered person's protected home address or unpublished telephone number] and remove the protected information from the Internet or where otherwise made available." N.J.S.A. 56:8-166.1(a)(2). The statute instructs that such notifications "shall" be "provide[d]" by the covered persons themselves, except in certain limited situations not applicable here (e.g., where a covered person is medically incapacitated or a minor). N.J.S.A. 56:8-166.1(a)(2), (d). The statute does not require any form of verification that the person seeking non-disclosure truly qualifies as a "covered person," however, but rather only requires the notification to state that the person providing it is in fact a covered person (or someone authorized to act on their behalf, where applicable). N.J.S.A. 56:8-166.1(a)(2).

While the statute ostensibly requires the recipient of a notification not to "disclose" a person's home address or unpublished phone number "on the Internet," it includes a sweeping definition of the term "disclose" that covers a far broader range of conduct than the ordinary meaning of the term encompasses. Specifically, the statute defines the term "disclose" to mean

> to solicit, sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, post, publish, distribute, circulate, disseminate, present, exhibit, advertise, or offer, and shall include making available or viewable within a searchable list or database, regardless of whether a search of such list or database is actually performed.

N.J.S.A. 56:8-166.1(d). Thus, on its face, the statute applies to virtually any type of transmission or transaction involving a covered person's information—even if the transmission or transaction is purely between two businesses, or even between two people within the *same* business. Further, the statute does not even stop at prohibiting all those forms of conduct broadly defined to constitute "disclosure," but also includes catchall language providing that the recipient of a notification shall not "otherwise make available" the covered person's information, without defining or limiting this phrase in any way.

This far-reaching prohibition is coupled with a rigid compliance deadline. Specifically, the statute provides that, "[u]pon notification," the recipient of the notification must comply with the non-disclosure request "not later than 10 business days following receipt thereof." N.J.S.A. 56:8-166.1(a)(1). The statute does not build any exceptions or flexibility into this deadline. For example, it takes no account of whether the notification is directed to a person or to an inbox designated for receiving such notifications, or whether the notification contains sufficient information for the business to identify the covered person's information in its records (e.g., the person's applicable username or the correct variant of the person's

name or address), or whether there are any extenuating circumstances that make it unreasonable to expect the recipient to process the notification within 10 business days—such as when tens of thousands of notifications are intentionally sent *en masse* within a short time period in a purposeful effort to frustrate timely compliance, as Atlas did here.

Failure to meet the statute's rigid compliance deadline in turn exposes companies to monetary damages, regardless of the circumstances. The statute provides that a "court *shall* award" "actual" damages that are "not less than" what the statute calls "liquidated damages" of "$1,000 for each violation of this act"—without regard to whether the "violation" involved intentional misconduct or even negligence by the defendant. N.J.S.A. 56:8-166.1(c)(1). Notably, this is a recent addition to the statute, enacted in 2023—merely six months before these Complaints were filed—together with the assignment provision on which Atlas is relying to bring this litigation. The damages provision reached its current form in several steps:

- As originally enacted in 2020, Daniel's Law permitted a covered person to seek only an injunction in the event of non-compliance with a non-

disclosure notification, and to recover fees and costs if successful, N.J.S.A. 56:8-166.2(2)(c) (2020).[2]

- In 2021, the statute was amended to provide that a court "may" award $1,000 in "liquidated damages" based on a violation of the notification provision—providing a court with discretion to award such damages where it deemed them warranted. N.J.S.A. 56:8-166.1(1)(c) (2021). At the same time, the legislature balanced this discretionary damages provision with a new requirement for a covered person to obtain "approval from the [New Jersey] Office of Information Privacy" before making a non-disclosure notification—thereby protecting against abusive requests. N.J.S.A. 56:8-166.1(a)(1) (2021).
- In 2023, however, the legislature removed the discretionary element of the damages provision by changing "may" to "shall." Yet it simultaneously

[2] At the time Daniel's Law was enacted, "liquidated damages" of $1,000 per violation were already available under a separate provision of law, unrelated to non-disclosure notifications submitted by covered persons, in the event of a disclosure of any law enforcement officer's home address or phone number in circumstances where "a reasonable person would believe" that doing so would cause harm. N.J.S.A. 56:8-166.1(1)(c) (2016). The legislature was clearly aware of this provision when it enacted Daniel's Law: As part of the enactment, that provision was amended to cover judges and prosecutors in addition to law enforcement officers. Yet the legislature did not incorporate any damages provision of any kind into the new notification-based provision. N.J.S.A. 56:8-166.2(1)(c) (2020).

eliminated the requirement that a covered person obtain approval from the Office of Information Privacy before making a non-disclosure notification.

The legislature did not explain the rationale for ***any*** of these changes. In particular, the legislative history contains no explanation of why the legislature ultimately considered a strict liability regime—unaccompanied by any governmental screening of notifications—to be necessary to effectuate the statute's aims, as opposed to injunctive relief or a discretionary fine. These changes appear only to have maximized the value of a potential extortive lawsuit by Atlas rather than to have done anything to increase the safety of covered persons.

2. The Statute Does Not Impose Similarly Stringent Requirements on Governmental Agencies Even Though Public Records Present Similar Safety Risks

The foregoing provisions—which apply to non-disclosure notifications made to private businesses—stand in marked contrast to the other provisions of Daniel's Law applicable to public agencies, which provide a mechanism for covered persons to seek "the redaction or nondisclosure of [their] home address" (but not phone number) from certain public records. N.J.S.A. 47:1B-2(a).

First, for a covered person to obtain redaction of public records, the request must first be "submitted to and approved by the Director of the Office of Information Privacy." *Id.* As noted above, the statute previously included a similar approval requirement for private non-disclosure requests, but that statutory provision was

removed in 2023, without explanation—eliminating a neutral, independent means of verifying that a requesting individual is in fact a covered person and an important check against abusive requests. *Compare* N.J.S.A. 56:8-166.1(a)(1) (2021), *with* N.J.S.A. 56:8-166.1(a)(1) (2023).

Second, even though the safety implications of the disclosure of a covered person's home address or phone number would presumably be the same regardless of whether disclosure is made by a public agency or a private business, public agencies—unlike private businesses—are not required to implement a non-disclosure request within 10 business days. Again, the request must be approved by the Office of Information Privacy first—and the statute imposes no deadline by which the Office of Information Privacy must act. Even after approval, public agencies have 30 days, rather than 10 days, to implement the approved request. *See* N.J.S.A. 47:1B-2(b). The statute does not provide any specific judicial remedy—much less "liquidated damages"—if a public agency fails to meet this (more generous) statutory deadline. And there is no ability for covered persons to require public agencies to cease disclosure of phone numbers at all.

Third, public agencies are allowed to use and share home address information in their ordinary course of business (and unpublished phone number information for any purpose), notwithstanding their receipt of non-disclosure requests, while the statute affords private businesses no such leeway. Thus, the statute provides that

"[a] public agency may share unredacted information with any vendor, contractor, or organization to carry out the purposes for which the public agency entered into an agreement with the vendor, contractor, or organization." N.J.S.A. 47:1B-3(a)(5). Likewise, the statute provides that it shall not be construed to "require redaction or nondisclosure of any information in any document, record, information, or database shared with or otherwise provided to any other government entity." N.J.S.A. 47:1B-3(b). By comparison, a *private* entity receiving a non-disclosure notice may not "give," "provide," "circulate," "disseminate," or "otherwise make available" a covered person's home address or unpublished phone number to anyone—*without exception*—even if the recipient is a vendor, contractor, or organization that has contracted with the entity, the "disclosure" is private (i.e., business-to-business), and the information is needed (and would only be used) to perform a contract.

3. The Statute Contains Substantial Exceptions to Non-Disclosure That Undercut Its Legislative Purpose

At the same time that Daniel's Law imposes sweeping prohibitions on private companies, accompanied by rigid deadlines and harsh penalties, it also contains significant exceptions to non-disclosure requirements—meaning that private businesses can be punished for failing to take down a covered person's information within a strict time limit, even though the same information remains readily accessible through other sources within the public domain.

Most significantly, the statute provides that records held by public agencies "evidencing any lien, judgement, or other encumbrance upon real or other property"—which encompasses mortgage records—are not subject to requests for redaction or non-disclosure. N.J.S.A. 47:1B-3(a)(4)(d). Similarly, a title insurance company, real estate broker, or title search company may receive from a public agency, unredacted, "a document affecting the title to real property" and then re-disclose the information in their ordinary course of business—even if they have received a non-disclosure notification from a covered person. N.J.S.A. 47:1B-3(a)(2); N.J.S.A. 56:8-166.1(e). The availability of mortgage and title records on the internet, where the records are searchable by name, can provide an easy way to find the home address of a covered person even if it has been taken down from other sources. For example, the home addresses of ***at least four of the six individually identified Plaintiffs*** can easily be looked up in property records presently made available on the internet by New Jersey county agencies, through databases that are searchable by name. *See* Mortgage, Ex. 2; Mortgage, Ex. 3; Notice of Settlement and Mortgage, Ex. 4 (address information has been redacted).[3]

[3] The Court may take judicial notice of these public records on a motion to dismiss. *See, e.g.*, *Anspach ex rel. Anspach v. City of Phila. Dep't of Public Health*, 503 F.3d 256, 273 n. 11 (3d Cir. 2007) ("Courts ruling on Rule 12(b)(6) motions may take judicial notice of public records."); *Stone v. JPMorgan Chase Bank, N.A.*,

Relatedly, Daniel's Law does not require a covered person to provide a non-disclosure request to public agencies before (or even after) providing a non-disclosure request to private businesses. A covered person's information can thus remain available online through governmental sources even when it is subject to a non-disclosure request and even when such a request has been made to private businesses, just as public records reflect here for four of the six individually identified Plaintiffs. And a covered person's information can even be publicized elsewhere by the covered person themselves—as they are not required to represent that they have refrained from self-publishing their information when they provide a non-disclosure notification to others.[4]

---

415 F. Supp. 3d 628, 631–32 (E.D. Pa. 2019) (taking judicial notice of mortgage assignment record that was publicly filed with county recorder of deeds).

[4] For example, some of the Plaintiffs have self-published some of the very information included in the non-disclosure notifications Atlas provided putatively on their behalf. For example, Plaintiff Maldonado lists his phone number in his public LinkedIn profile, *see* Ex. 5, as well as on websites promoting his real estate company, *see* Ex. 6. Plaintiff Colligan listed his phone number in a press release, Ex. 7, and in a publicly available retirement party announcement, Ex. 8. And Plaintiff Andreyev made one of his phone numbers publicly available via his wife's corporate web page, *see* Ex. 9.

B. Atlas's Attempt to Exploit the Excessive Breadth and Punitiveness of Daniel's Law

In 2023—again, at the same time the language of the "liquidated damages" provision was changed from "may" to "shall"—Daniel's Law was curiously amended to include an unusual provision allowing for the "assignment" of civil claims under the statute. The provision now states that a person in violation of the statute "shall be liable to the covered person *or the covered person's assignee*, who may bring a civil action in the Superior Court." N.J.S.A. 56:8-166.1(b) (2023) (emphasis added). The amendment was made with no rationale or explanation. Notably, attorneys from Genova Burns LLC (who are now at Pem Law LLP)—one of the law firms representing Atlas—reported they were lobbyists for Atlas in New Jersey in April 2023, four months before the assignment provision was enacted. *See* Genova Burns Annual Report of Governmental Affairs Agent, Ex. 10.

Atlas was incorporated in April 2021, shortly after the original version of Daniel's Law was passed. *See* Atlas Data Privacy Corporation Certificate of Authority, Ex. 11. Atlas claims to offer services to individuals aimed at removing their sensitive identifying information from the internet. *See* Atlas, https://www.atlas.net, Ex. 12. According to the Complaints filed here, Atlas "works with and provides access to its platform to members of the New Jersey State Policemen's Benevolent Association ("NJSPBA"), the Metropolitan Transportation

Authority Police Benevolent Association, New Jersey PBA Local 105, and the New Jersey State Troopers Fraternal Association, among others." Compl. ¶ 31.

Atlas solicited members from these organizations to sign up for Atlas's services at least as early as April 5, 2023. *See The Right to Privacy and to Attend the Mini Convention*, N.J. COPS MAG. (Apr. 5, 2023), http://njcopsmagazine.com/the-right-to-privacy-and-to-attend-the-mini-convention ("The time is now to sign up for protection under Daniel's Law through Atlas Privacy."), Ex. 13. As part of Atlas's terms of service in effect at the time, anyone who signed up for its services agreed in advance to "irrevocably assign[] to [Atlas] all of [their] rights to bring a claim (and seek damages …) for violations of [their] rights under [Daniel's Law]." See Atlas Terms of Service at 6, Ex. 14 ("Terms").[5] The Terms provided that Atlas could unilaterally "trigger" this assignment by sending "Assignment Confirmations" to the covered persons if, at its "discretion,"

[5] On April 18, 2024, the Court ordered the Plaintiffs to produce the Terms as part of the evidence reflecting the assignments allegedly made to Atlas. ECF No. 28. Because the alleged assignments, as well as Atlas's signup process, are incorporated by reference in Atlas's Complaints, *see* Compl. ¶¶ 32–36, the Court can consider the Terms on this motion to dismiss. *See Pension Ben. Guar. Corp. v. White Consol. Indus., Inc.*, 998 F.2d 1192, 1196 (3d Cir. 1993) ("[A] court may consider an undisputedly authentic document that a defendant attaches as an exhibit to a motion to dismiss if the plaintiff's claims are based on the document.").

Atlas decided to bring "civil litigation whereby individual claims are aggregated and prosecuted by Atlas." *See id.*[6]

Even though Atlas solicited assignors *for months* over the course of 2023, it did not send Defendants purported non-disclosure notifications on behalf of these individuals as they signed up—as one would expect had Atlas truly had their safety at heart. Instead, Atlas *waited months* until it had amassed more than 19,000 assignors, and only then began sending purported non-disclosure notifications on their behalf during the December 2023 holiday season, in enormous email blasts of thousands of emails at a time, directed at well over 100 companies.[7] Compl. ¶ 51 (alleging that non-disclosure requests for "all of the Covered Persons (who assigned claims to Atlas))" were sent "using AtlasMail" "[s]tarting on or about December 30, 2023").[8]

---

[6] Defendants do not concede that there has been a lawful or valid assignment to Atlas of any covered person's purported claims.

[7] As any reasonable person would know—particularly Atlas, which purports to provide data privacy services—such email blasts create a risk of triggering spam filters that would prevent the information from being successfully delivered.

[8] The Complaints brought against Defendants specify different start dates for the email blasts directed at each respective Defendant or group of Defendants. *See, e.g.*, Compl. ¶ 51, *Atlas Data Privacy Corp. v. CoStar Group Inc.*, No. 1:24-cv-04111-HB (D.N.J) ("CoStar Complaint"); ("Starting on or about December 28, 2023…"); Compl. ¶ 53, *Atlas Data Privacy Corp. v. TransUnion*, No. 1:24-cv-04288-HB (D.N.J) ("TransUnion Complaint") ("Starting on or about January 2, 2024…"). However, the start dates all are from late December 2023 or later—months after Atlas began soliciting assignors.

While the Complaints filed against Defendants allege in conclusory fashion that the "Covered Persons sent Defendants a takedown notice," Compl. ¶ 34; *see also* ¶ 51, it is abundantly clear that the notifications at issue were sent *by Atlas*, putatively *on behalf* of covered persons. The requests all followed the same template and all originated from email addresses associated with "Atlas Mail" ("@AtlasMail.com"), Compl. ¶¶ 33–35, and they were sent to each Defendant in consolidated email blasts, with the individual emails within each blast sent within seconds of one another.[9] Obviously, 19,000+ covered persons did not separately send emails at the same time; Atlas was necessarily the one pressing the button.[10]

Beginning in February 2024, Atlas (as alleged assignee for over 19,000 covered persons) and several individual Plaintiffs brought nearly identical suits

---

[9] A spreadsheet reflecting the timestamps of a sample of the emails directed to one Defendant reflects this pattern. *See* Ex. 15. Because the emails sent from Atlas Mail are incorporated by reference into the Complaints, the Court may consider this exhibit on a motion to dismiss. *See Buck v. Hampton Twp. Sch. Dist.,* 452 F.3d 256, 260 (3d Cir. 2006) ("In evaluating a motion to dismiss, we may consider documents that are attached to or submitted with the complaint, and any matters incorporated by reference or integral to the claim …." (cleaned up)).

[10] This is despite the fact that the assignment provision, added in 2023, did nothing to change the statute's requirement that a non-disclosure notification must be "provided" by a covered person *themself*—save in limited circumstances not alleged to be applicable here. *See* N.J.S.A. 56:8-166:1(a)(2), (c). Nothing in the statute, even as most recently amended, allows a putative *assignee* to provide a non-disclosure request on behalf of an assignor, which is precisely what Atlas did. Defendants reserve all rights to challenge the validity of the purported non-disclosure notifications at issue at a later time.

against 143 companies that received Atlas's email blasts, including the Defendants, in New Jersey Superior Court. Subsequently, 73 of these cases were removed to federal court. The Complaints allege violations of Daniel's Law for failure to take down the personal information of the thousands of covered persons at issue within 10 business days of receiving notifications. Compl. ¶¶ 51, 59. The Complaints seek all forms of relief permitted by Daniel's Law, including "liquidated damages" and even punitive damages. Compl. ¶ 61.

C. The Parties

1. Plaintiffs

The lead Plaintiff in this litigation is Atlas, which brings suit as the purported assignee of over 19,000 covered persons' claims under Daniel's Law.[11] Compl. ¶ 26. Having sent thousands of purported non-disclosure notifications on behalf of these "assignors," Atlas now seeks millions of dollars from each Defendant. *Id.* ¶ 61.

The Complaints also name eight current and former law enforcement officials (including two Jane Does) as individual Plaintiffs, including current and former leaders of the NJSPBA. Compl. ¶¶ 15–18, 22–24.

[11] Each Complaint is brought by Atlas on behalf of at least 10,000 alleged assignors, and in some cases more than 19,000. The exact number varies by Complaint.

2. The Defendants

There are over 105 Defendants in the cases before this Court, representing a wide variety of industries and services.[12] They include, among other entities, real estate businesses;[13] direct-mailing and marketing companies;[14] data brokers;[15] entities that provide fundraising solutions to charities and other nonprofits;[16] credit

---

[12] The Court may consider the websites below, Exs. 16-30, as they are incorporated by reference in the Complaints. *See, e.g.*, *Kickflip, Inc. v. Facebook, Inc*., 999 F. Supp. 2d 677, 682 (D. Del. 2013) (considering website pages that were "directly cited in the Complaint by their internet addresses").

[13] *See, e.g.*, CoStar, https://www.costar.com/ (providing a "commercial real estate information, analytics and news platform"), *cited in* CoStar Complaint ¶ 39; Lightbox, https://www.lightboxre.com/ (providing services to "empower decision makers in the commercial real estate market"), *cited in* Compl. ¶ 39, *Atlas Data Privacy Corp. v. Lightbox Parent, L.P.,* No. 1:24-cv-04105-HB (D.N.J) ("Lightbox Complaint"); Zillow, https://www.zillow.com/ (providing options to "[f]inance a home," "[b]uy a home," or "[r]ent a home"), *cited in* Compl. ¶ 39, *Atlas Data Privacy Corp. v. Zillow, Inc.*, No. 1:24-cv-04256-HB (D.N.J); RE/MAX, https://www.remax.com/ ("The right time to move is when you're with the right agent—nobody sells more real estate than RE/MAX."), *cited in* Compl. ¶ 39, *Atlas Data Privacy Corp. v. RE/MAX LLC,* No. 1:24-cv-04114-HB (D.N.J) ("RE/MAX Complaint").

[14] *See, e.g.*, DM Group, https://www.dmgroup.com/ ("[W]e offer a full range of services to help our clients achieve their marketing goals."), *cited in* Compl. ¶ 33, *Atlas Data Privacy Corp. v. DM Group Inc.*, No. 1:24-cv 04075-HB (D.N.J).

[15] *See, e.g.*, Axicom, https://www.acxiom.com/ (enabling businesses to "integrate our data and identity solutions to help brands build the right data foundation for improved marketing performance."), *cited in* Compl. ¶ 40, *Atlas Data Privacy Corp. v. Axciom LLC*, No. 1:24-cv-04107-HB (D.N.J).

[16] *See* Blackbaud, https://www.blackbaud.com/ (offering "[s]oftware built for fundraising, nonprofit accounting, education, CSR and more"), *cited in* Compl. ¶ 39.

reporting agencies regulated under the Fair Credit Reporting Act;[17] and entities that provide voter information to political campaigns, government offices, news media outlets, and universities.[18]

The panoply of businesses targeted in the Complaints only underscores the breadth of conduct that an abusive plaintiff like Atlas could argue falls within the expansive terms of Daniel's Law.[19] Many Defendants targeted in these Complaints do not make home addresses or phone numbers publicly searchable by name or otherwise disclose this information on the internet. For example, numerous Defendants provide data only to other businesses, not to the general public. *See, e.g.*, Oracle, https://www.oracle.com/ (explaining that its products are for "business[es]"

---

[17] *See* TransUnion, https://www.transunion.com/ (providing credit reporting services), *cited in* TransUnion Complaint ¶ 40; Equifax, https://www.equifax.com/ (similar), *cited in* Compl. ¶ 40, *Atlas Data Privacy Corp. v. Equifax Inc.*, No. 1:24-cv-04298-HB (D.N.J); Innovis, https://innovis.com/ (similar), *cited in* Compl. ¶ 39, *Atlas Data Privacy Corp. v. Innovis Data Solutions Inc.*, No. 1:24-cv-04176-HB (D.N.J).

[18] *See, e.g.*, E-Merges.com, Inc., https://www.emerges.com/ (providing "registered voter lists to political campaigns, pollsters, committees, universities, and researchers"), *cited in* Compl. ¶ 39, *Atlas Data Privacy Corp. v. E-Merges.com Inc.*, No. 1:24-cv-04434-HB (D.N.J) ("E-Merges Complaint").

[19] Defendants reserve all rights to argue, at a later date, that their conduct is not covered by Daniel's Law, whether because it does not fall within the statutory definition of "disclose," or because it falls within one of the statutory exceptions, or for any other reason.

and "enterprise[s]")[20]; Lightbox, https://www.lightboxre.com/ (explaining that it provides data to "decision makers in the commercial real estate market"); PostcardMania, https://www.postcardmania.com/products-services/ (explaining that it offers "postcard marketing services" for businesses).[21] As another example, some businesses have services that provide information about *an already identified* address or phone number, but do not enable a user to *find* someone's address or phone number by looking up their name. *See, e.g.*, Homes.com, https://www.homes.com/ (allowing search by "place," but not by name).[22]

III. LEGAL STANDARD

A Rule 12(b)(6) motion allows "a court to dismiss a claim on the basis of a dispositive issue of law" before the parties become mired in "needless discovery and factfinding." *Neitzke v. Williams*, 490 U.S. 319, 327 (1989). In general, a court considering such a motion may not "go beyond the facts alleged in the Complaint and the documents on which the claims made therein are based." *Bruni v. City of Pittsburgh*, 824 F.3d 353, 360 (3d Cir. 2016) (alterations in original). "The court

---

[20] *Cited in* Compl. ¶ 41, *Atlas Data Privacy Corp. v. Oracle International Corp.*, No. 1:24-cv-04112-HB (D.N.J) ("Oracle Complaint").

[21] *Cited in* Joy Rockwell Complaint ¶ 39.

[22] *Cited in* CoStar Complaint ¶ 39.

may, however, rely upon 'exhibits attached to the complaint and matters of public record.'" *Id.* (citation omitted).

IV. ARGUMENT

"The First Amendment, applicable to the States through the Fourteenth Amendment, prohibits laws that abridge the freedom of speech." *Nat'l Inst. of Fam. & Life Advocs. v. Becerra*, 585 U.S. 755, 766 (2018). The New Jersey State Constitution likewise provides that "[n]o law shall be passed to restrain or abridge the liberty of speech or of the press." N.J. Const. art. I, ¶ 6. "The 'State Constitution's free speech clause is generally interpreted as co-extensive with the First Amendment,'" and in fact "affords greater protection than federal law in certain areas relating to free speech." *Usachenok v. Dep't of the Treasury*, 313 A.3d 53, 60 (N.J. 2024) (citations omitted).

The speech protected by the First Amendment sweeps broadly. *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011). Very few categories of speech "lie outside the bounds of the First Amendment's protection." *Counterman v. Colorado*, 600 U.S. 66, 72 (2023). None of those narrow categories—"incitement," "defamation," "obscenity," and "true threats"—is at issue here. *Id.* at 73–74. Rather, Daniel's Law restricts the "dissemination of information"—i.e., address and phone number information—which under settled law constitutes "speech within the meaning of the First Amendment." *Sorrell*, 564 U.S. at 570. Although Daniel's Law was intended

to serve the state's interest in enhancing the safety of judges, law enforcement officers, and other public officials, it is not sufficiently tailored to advancing that purpose, as required by the Constitution, and it is also unconstitutionally vague in critical respects.

A. Daniel's Law Is a Content-Based Speech Restriction Subject to Strict Scrutiny

Content-based restrictions on speech are "presumptively unconstitutional." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015). In general, such restrictions can overcome the presumption of unconstitutionality only by satisfying "strict scrutiny," which requires "the government [to] prove[] that [the restrictions] are narrowly tailored to serve compelling state interests." *Id.* at 164 (citations omitted). This is a "daunting burden," *Schrader v. Dist. Att'y of York Cnty.*, 74 F.4th 120, 127 (3d Cir. 2023). It is thus "rare that a regulation restricting speech because of its content will ever be permissible." *Brown v. Entm't. Merchs. Ass'n*, 564 U.S. 786, 799 (2011) (citation omitted).

Content-based restrictions are those "that target speech based on its communicative content." *Reed*, 576 U.S. at 163. Any law that is "targeted at specific subject matter is content based even if it does not discriminate among viewpoints within that subject matter." *Id.* at 169. Laws that impose "'restraints on the way in which [certain] information might be used' or disseminated'" are prime examples of content-based restrictions. *Sorrell*, 564 U.S. at 568 (citation omitted).

The Ninth Circuit, for example, recently held that a California state law restricting the "dissemination" of "'date of birth or age information'" was a content-based restriction. *IMDb.com v. Becerra*, 962 F.3d 1111, 1120 (9th Cir. 2020) (quoting Cal. Civ. Code § 1798.83.5(b)).

Daniel's Law is plainly a content-based restriction. By prohibiting persons from "disclos[ing]" or "mak[ing] available" a certain type of information—i.e, "the home address or unpublished home telephone number of any covered person," N.J.S.A. 56:8-166.1(a)(1)—the statute restricts speech based on its communicative content. In other words, the statute "asks what a person said" and, depending on the answer, either allows or prohibits the speech. *Reed*, 576 U.S. at 169. That is the hallmark of a content-based restriction. *Id.*

Other courts have concluded that statutes designed to restrict dissemination of personal information of government officials are content-based speech restrictions. In *Brayshaw v. City of Tallahassee*, for example, the district court concluded that a state law prohibiting the malicious "publish[ing] or disseminat[ion]" of "the residence address or telephone number of any law enforcement officer" was "clearly content-based, as it restricts speech based [on] its subject." 709 F. Supp. 2d 1244, 1249–50 (N.D. Fla. 2010). Likewise, in *Sheehan v. Gregoire*, the district court found that a prohibition on maliciously disseminating the personal information of law enforcement or court personnel was content-based, as it regulated speech "based

solely on the subjects addressed by that speech—whether the information identifies law enforcement-related, corrections officer-related, or court-related employees." 272 F. Supp. 2d 1135, 1146 (W.D. Wash. 2003). And in *Publius v. Boyer-Vine*, the district court found that a statute allowing certain government officials to demand takedowns of their home address or phone number was "content-based on its face" because "it applies only to speech that contains certain content—the 'home address or telephone number of any elected or appointed [California] official.'" 237 F. Supp. 3d 997, 1012–13 (E.D. Cal. 2017) (citations omitted).

A narrow exception to the general rule described above has traditionally been applied to what the Supreme Court has referred to as "commercial speech." *See Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 563 (1980). But "commercial speech" refers to "speech that does no more than propose a commercial transaction." *Harris v. Quinn*, 573 U.S. 616, 648 (2014). The speech restricted by Daniel's Law does not propose a commercial transaction at all. While Defendants may have an "economic motivation" in the restricted speech, such motivation is "clearly [] insufficient by itself to turn [the speech] into commercial speech." *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 67 (1983). Indeed, courts routinely hold that address and phone number information, even when disseminated by a for-profit business, constitutes non-commercial speech. *See, e.g.*, *Vrdolyak v. Avvo, Inc.*, 206 F. Supp. 3d 1384, 1386, 1389 (N.D. Ill. 2016) (holding

that attorney profile website containing address and phone number information is non-commercial speech); *Dex Media W., Inc. v. City of Seattle*, 696 F.3d 952, 962 (9th Cir. 2012) (holding that phone numbers and community information in telephone directory constitute non-commercial speech); *IMDb.com*, 962 F.3d at 1122 (holding that online database containing age and date of birth information was "encyclopedic, not transactional," and therefore not commercial speech).

Because Daniel's Law is a content-based restriction on non-commercial speech, it must be analyzed under strict scrutiny.

B. Daniel's Law Cannot Satisfy Strict Scrutiny

Under strict scrutiny, a content-based restriction must "further[] a compelling interest." *Reed*, 576 U.S. at 171 (citation omitted). Here, Daniel's Law was enacted to "enhance the safety and security of certain public officials in the justice system" and thereby "foster the ability of these public servants . . . to carry out their official duties without fear of personal reprisal." N.J.S.A. 56:8-166.3. However, even assuming this interest is compelling, strict scrutiny demands that the *means* chosen by the legislature must be "narrowly tailored" to achieve this interest. *Reed*, 576 U.S. at 171. In other words, the legislature must "curtail speech as little as possible" in order to accomplish its goal. *Camp Hill Borough Republican Ass'n v. Borough of Camp Hill*, 101 F.4th 266, 271 (3d Cir. 2024).

Multiple district courts across the country have found statutes restricting disclosure of government officials' personal information to be unconstitutional based on tailoring deficiencies. *See Publius*, 237 F. Supp. 3d at 1019 (granting preliminary injunction to block enforcement of statute allowing government officials to request takedown of address or phone number information, because even assuming state had compelling interest in protecting officials' safety, "the statute is not narrowly tailored to further that interest"); *Brayshaw*, 709 F. Supp. 2d at 1247, 1249 (concluding that a state law prohibiting the "publish[ing] or disseminat[ion]" of "the residence address or telephone number of any law enforcement officer" was unconstitutional because it was not "narrowly tailored" to serve "the state interest of protecting police officers from harm"); *Sheehan*, 272 F. Supp. 2d at 1139, 1146 (finding law prohibiting any "person or organization" to "sell, trade, give, publish, distribute, or otherwise release" address or phone number information of members of law enforcement and certain other public officials was not "narrowly tailored").

Daniel's Law similarly fails because it restricts substantially more speech than necessary to achieve its goal of enhancing the safety of public officials. As explained below, the statute is both substantially over-inclusive and under-inclusive, and disregards "available, effective, alternatives" that curtail far less speech and that the legislature could have enacted instead. *Schrader*, 74 F.4th at 127.

1. Daniel's Law Restricts Significantly More Speech Than Necessary to Protect the Government's Interest

Daniel's Law prohibits a wide array of conduct that does not implicate safety concerns. The statute therefore is not sufficiently tailored to achieve the state's interest in enhancing the safety of public officials. *See, e.g.*, *Brown*, 564 U.S. at 804 (2011) (finding restriction on children's access to violent video games "vastly overinclusive" as compared to "the Act's purported aid to parental authority"); *ACLU v. Ashcroft*, 322 F.3d 240, 257 (3d Cir. 2003), *aff'd*, 542 U.S. 656 (2004) (finding regulation of pornography, aimed at protecting minors, overbroad because it also "prohibits a wide range of protected expression").

a) The Definition of "Disclose" Restricts More Speech Than Is Necessary

The problems with Daniel's Law begin with its sweeping definition of "disclose." As explained above, the term "disclose" is given an exceedingly broad scope that, on its face, encompasses many uses of address or phone number information that have no apparent connection to the safety concerns motivating the statute. The term is defined to mean "solicit, sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, post, publish, distribute, circulate, disseminate, present, exhibit, advertise, or offer," and includes "making available or viewable within a searchable list or database, *regardless* of whether a search of such list or database is actually performed." N.J.S.A. 56:8-166.1(d) (emphasis added). Nothing in the

statute limits the prohibition to disclosures to the public, as opposed to purely private disclosures to other businesses or within a business. Even the fact that the disclosure must occur "on the Internet," N.J.S.A. 56:8-166.1(a)(1), is not a significant limitation, as all manner of activity occurs over the internet—including email, messaging, remote access to corporate networks, cloud hosting, business applications, and countless other forms of communication and data processing.

For example, under the broad definition of "disclose," the statute could prohibit a business or entity from:

- "selling" (or even "offering") address information to another business for use in mail-marketing campaigns—even if the underlying contract disallows use of the information for any other purpose; [23]
- "disseminating" voter addresses to political campaigns or advocacy organizations, even when the applicable terms of use forbid further dissemination;[24]

---

[23] Notably, the Daniel's Law provisions addressed to public agencies allow those agencies to share covered persons' information with contractors or other agencies as part of their ordinary course of business, N.J.S.A. 47:1B-3(5)—which only underscores the overinclusive nature of the provisions addressed to private businesses, which operate to prohibit such harmless conduct.

[24] By restricting campaigns from using, disclosing, and sharing voter information, the statute infringes on both campaigns' and voters' rights to engage in protected political speech. *See Voter Reference Found., LLC v. Balderas*, 616 F. Supp. 3d

- "giving" a customer address list to an acquiring company in a merger, even if the acquiring company is simply taking on the target company's information;
- "providing" a covered person's address or phone number to a vendor—e.g., a shipper used by an online store—even if the vendor needs the information to perform its contract with the store;
- "transferring" a person's address to a cloud storage service that the business uses to store its customer information; and
- merely *maintaining* an *internal* database containing a covered person's information that the company's employees can access remotely, insofar as that would make the information "available or viewable" to the employees "on the Internet" in "a searchable list or database, regardless of whether a search of such list or database is actually performed."

The statute's indiscriminate definition of "disclose" is highly problematic from a constitutional perspective. It is difficult to understand—and the legislature failed to explain—how prohibiting these sorts of "disclosures" would meaningfully and directly advance the state's interest in the safety of public officials. Even worse,

---

1132, 1261 (D.N.M. 2022) (voter rolls are "the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs" (citation omitted)).

the statute goes *beyond* this definition and prohibits "otherwise mak[ing] available" covered persons' information—adding even greater sweep to the statute and correspondingly greater question as to how it advances safety. This "overinclusive" breadth of the statute violates the First Amendment. *Brayshaw*, 709 F. Supp. 2d at 1249–50 (finding statute restricting disclosure of law enforcement information "overinclusive in proscribing speech that is not a true threat"); *see generally Simon & Schuster, Inc. v. Members of New York State Crime Victims Bd.*, 502 U.S. 105, 120–21 (1991) (declaring statute "significantly overinclusive" because, among other things, statute's definition of "person convicted of crime" swept in range of behavior implicating "little if any [state] interest"); *Carey v. Wolnitzek*, 614 F.3d 189, 205 (6th Cir. 2010) (finding narrow-tailoring problem where statute's definition of "solicitation" encompassed "methods of solicitation" that "present little or no risk" to the purported state interest); *Ams. for Prosperity v. Grewal*, No. 19-cv-14228-BRM-LHG, 2019 WL 4855853, at *17 (D.N.J. Oct. 2, 2019) (granting preliminary injunction of campaign finance law on First Amendment grounds because "the broad inclusiveness of the Act's definition of media bears little relation to what media are actually used" for electioneering purposes, and as a result "practically any media spending appears to trigger the Act's disclosure and reporting regime").

The statute's tailoring deficiencies continue with its seemingly categorical prohibition on disclosing a covered person's home address or phone number—even

when the disclosure does not include any information linking the address or phone number *to the covered person*. *See* N.J.S.A. 56:8-166.1(a)(1) (imposing blanket restriction on any "disclosure" of "the home address or unpublished home telephone number of any covered person"). This would appear to imply, for example, that were Google to receive a non-disclosure notification from a covered person, it would have to remove the individual's address from Google Maps, even though the address would not appear in any way that links it to the covered person. Courts routinely find speech restrictions unconstitutional when they encompass behavior that has no significant nexus to the state's purported interest. *See Brown*, 564 U.S. at 804; *ACLU*, 322 F.3d at 267–68.[25]

[25] Compounding the statute's tailoring problems, Daniel's Law does not include any exception for reporting, news-gathering, or other activities intended to inform the public on matters of public concern. Courts have held that publication of the type of information at issue here—individuals' home addresses and phone numbers—can be in the public interest in certain circumstances. *See, e.g.*, *Publius*, 237 F. Supp. 3d at 1014; *Brayshaw*, 709 F. Supp. 2d at 1249. Yet Daniel's Law makes no accommodation for such situations, even where the information is obtained from public sources. *See Bartnicki v. Vopper*, 532 U.S. 514, 533–34 (2001) (laws that "impose[] sanctions on the publication of truthful information of public concern" implicate the "core purposes of the First Amendment"); *Bowley v. City of Uniontown Police Dep't*, 404 F.3d 783, 789 (3d Cir. 2005) ("[W]hen the government is ultimately responsible for the disclosure of information, imposing civil liability upon a newspaper for the subsequent publication of that information is not the most narrowly tailored means of serving any purported interest.").

b) The Lack of a Verification Process Restricts More Speech Than Necessary

The statute's tailoring problems are exacerbated by the lack of any process to verify whether a purported "covered person" is indeed a "covered person" who is entitled to the statute's protections. Absent such a process, the statute contains no means to ensure that its protections—and the concomitant restrictions on speech—are reserved for those individuals whom the statute was intended to protect. In contrast, the process for requesting non-disclosure of covered information from *public agency* sources includes such a verification requirement, as it makes fulfilment of non-disclosure requests contingent on seeking and receiving approval from the Office of Information Privacy. As explained above, prior to the most recent amendments to Daniel's Law, there was a similar requirement for non-disclosure requests directed to private persons or entities, but in 2023 the statute was amended—without any explanation—to *remove* that verification requirement and its protections, again unnecessarily extending the statute's sweep.

The state's interest in protecting the addresses and phone numbers of "covered persons" is the same whether a private person or business possesses the information or whether a government agency does. There is thus no good reason to impose a verification requirement only for requests to government agencies. And the fact that the process for requesting nondisclosure from government agencies includes a verification requirement precludes any argument that a similar requirement for non-

disclosure requests directed to private companies would undermine the state's safety interests. *See Publius*, 237 F. Supp. 3d at 1019 (finding that statute allowing government officials to request takedown of address or phone number information was not narrowly tailored because, among other things, it did "not require that the threat be credible or that a third-party review whether the official's request is well-founded" (internal citations omitted)).

The potential for improper chilling of protected speech based on the lack of a verification requirement is particularly worrisome given the legislature's decision to amend Daniel's Law in 2023 to allow for the "assignment" of claims. 2023 NJ Sess. Law Serv. Ch. 113 (WEST); *supra* at 13. The combination of the lack of a verification requirement with the ability to easily assign claims to opportunistic plaintiffs' lawyers incentivizes potentially abusive requests, utterly divorced from the core concerns of the statute. Yet, Defendants and others have no choice but to quickly comply with any requests received or risk lawsuits seeking to impose extensive civil liability. That chills far more speech than is necessary to achieve the state's interest in enhancing the safety of public officials.

c) The "Liquidated Damages" Provision Restricts More Speech Than Is Necessary

Finally, Daniel's Law goes further than necessary in providing that a court "shall" award "actual damages, but not less than liquidated damages computed at the rate of $1,000 for each violation of this act." N.J.S.A. 56:8-166.1(c)(1). This

provision does not merely apply to the intentional or negligent disregard of a non-disclosure notification; rather by its terms it applies to any "violation" of the statute, even if purely technical and inadvertent, and even if *induced by the plaintiff themself*, as Atlas has sought to do here. N.J.S.A. 56:8-166.1(c)(1).

The imposition of a harshly punitive remedy where a lesser remedy is sufficient to achieve the state's interest further highlights the legislature's insensitivity to free speech concerns and is relevant to the First Amendment analysis. *Schrader*, 74 F.4th at 128. Just last year, the Third Circuit disallowed a criminal prosecution for violation of a law prohibiting the publication of information from a government database, when the district attorney "offered little more than assertion and conjecture to support [his] claim that without criminal sanctions the objectives of [the law] would be seriously undermined." *Id.* (quoting *Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829, 841 (1978)) (alterations in original). In the Third Circuit's view, the availability of less punitive measures—for example, issuing a protective order preventing the sharing of the information at issue—doomed the state's attempt to impose the harsher consequence of criminal sanctions. *Id.*

The same logic applies to the harsh and inflexible damages provision at issue here. The objectives of Daniel's Law would be similarly served if the remedy for a civil violation were an injunction (like the protective order in *Schrader*), instead of a "liquidated damages" provision triggered by a short deadline, which takes no

account of whether the defendant is at fault for any failure to meet it. The legislature was clearly aware of less punitive alternatives. As originally enacted, the notification provision of Daniel's Law only provided for an injunction plus an award of fees and costs in the event of non-compliance, N.J.S.A. 56:8-166.2(2)(c) (2020); and even when the 2021 amendments introduced the possibility of "liquidated damages" in the notification provision, the statute provided only that a court "may" award such damages, leaving imposition to the sound discretion of the judge, N.J.S.A. 56:8-166.2(1)(c) (2021). No explanation was provided for the subsequent amendment in 2023 that changed "may" to "shall." Moreover, the legislature was also aware of a pre-existing provision of New Jersey law that made "liquidated damages" available for disclosure of certain personal information of law enforcement officers under circumstances where "a reasonable person would believe that doing so would cause harm." *See supra* n.2 (citing N.J.S.A. 56:8-166.1(1)(c) (2016)). Yet the liquidated damages provision of the notification provision of Daniel's Law has no nexus to such circumstances. No explanation was given in 2023 for why the legislature provided for "liquidated damages" in the notification provision in the absence of such belief.

All this "raise[s] concern that [the state] has too readily foregone options that could serve its interests just as well, without substantially burdening the kind of speech in which petitioners wish to engage." *McCullen v. Coakley*, 573 U.S. 464,

490 (2014). Indeed, the district court in *Publius* found a statute similar to Daniel's Law unconstitutional in part on the ground that the statute imposed mandatory attorney's fees and costs in the event that a defendant failed to timely comply with a covered official's request to take down the official's address or phone number information. 237 F. Supp. 3d at 1019–20. Even though only *attorney's fees and costs* were imposed by the statute at issue there, the court found that such "automatic liability" would have a "chilling effect on First Amendment rights" and compounded the narrow-tailoring concerns raised by the statute. *Id.* (citation omitted). This reasoning applies with even more force here, where so-called "liquidated damages" are available *in addition to* fees and costs.

* * *

In sum, by its plain terms, Daniel's Law prohibits broad categories of behavior that do not significantly implicate safety concerns. It also chills more speech than necessary by failing to include any verification mechanism and by providing for "liquidated damages" for violations. Thus, the statute is significantly over-inclusive and is insufficiently tailored to achieve its stated interest in enhancing the safety of public officials, and therefore fails strict scrutiny.

2. Daniel's Law Does Not Materially Advance the State's Safety Interests

Daniel's Law fails constitutional scrutiny for another reason. Not only does the law capture too *much* speech, it also captures too little, as the law allows many

entities, including public agencies, to continue publishing the same information that it punishes others for providing. These contradictions and holes in the statute's coverage imply that, as currently constructed, Daniel's Law is not effectively designed to reduce danger to public officials.

As the Supreme Court has noted, the "[u]nderinclusiveness" of a speech restriction is evidence "that a law does not actually *advance* a compelling interest." *Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 449 (2015); *see Yim v. City of Seattle*, 63 F.4th 783, 795 (9th Cir. 2023) ("[A] statute cannot meaningfully advance the government's stated interests if it contains exceptions that 'undermine and counteract those goals" (citation omitted)). Based on this principle, the Supreme Court in *Smith v. Daily Mail Publishing Company* struck down a statute prohibiting newspapers from releasing the names of juvenile defendants, when that prohibition did not extend to electronic media. 443 U.S. 97, 104-05 (1979). In light of the gaping hole in the statute's coverage, the Court concluded that the law "did not advance its stated purpose of protecting youth privacy." *Williams-Yulee*, 575 U.S. at 449 (summarizing *Daily Mail Publ'g*).

Daniel's Law suffers from similar under-inclusiveness concerns. For starters, the statute requires a private business or individual receiving a non-disclosure request to comply within 10 business days—regardless of whether the covered information will remain readily available in public records after that deadline.

Although Daniel's Law includes a separate process for removing certain covered information from public sources, *see* N.J.S.A. 47:1B-1–3, nothing requires a covered person to take advantage of that process before (or even after) sending a non-disclosure request to a business or a private person. In fact, the names and addresses of ***at least four of the individually identified Plaintiffs*** can readily be found online through name-based lookups of state property records. *See* Exs. 2–4.

Because many businesses obtain information about individuals' names, addresses, and phone numbers *from* New Jersey public agencies, which Daniel's Law does *not* require to remove information in parallel with any non-disclosure notification requests made to private businesses, the law is self-defeating. That under-inclusiveness contributes to the unconstitutionality of the statute. "[W]here the government has made certain information publicly available, it is highly anomalous to sanction persons other than the source of its release." *Florida Star v. B.J.F.*, 491 U.S. 524, 535 (1989); *see also Ostergren v. Cuccinelli*, 615 F.3d 263, 286–87 (4th Cir. 2010) ("We cannot conclude that prohibiting [the defendant] from posting public records online would be narrowly tailored to protecting individual privacy when Virginia currently makes those same records available …."); *Publius*, 237 F. Supp. 3d at 1020–21 (finding statute under-inclusive insofar as it proscribed dissemination of a covered official's home address and phone number "regardless

of the extent to which it is available or disseminated elsewhere"); *Brayshaw*, 709 F. Supp. 2d at 1250 (similar); *Sheehan*, 272 F. Supp. 2d at 1147 (similar).[26]

What is more, large categories of information—most significantly, "records evidencing any lien, judgement, or other encumbrance upon real or other property"—are not at all subject to redaction or non-disclosure under the statute. N.J.S.A. 47:1B-3(a)(4)(d). Thus, even if a covered person *does* make non-disclosure notifications to both private entities and public agencies, their information could still be made available through these real estate records, in an online form searchable by name (like the property records containing the individual Plaintiffs' information). Under these circumstances, prohibiting the "dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act." *Fla. Star*, 491 U.S. at 535. Where "the government has failed to police itself in disseminating information," the imposition of a restriction on the dissemination of similar information by private entities "can hardly

[26] Moreover, the private enforcement regime of Daniel's Law can result in a covered person's information remaining available on some websites but not on others, where covered persons themselves choose to self-publish the information and fail to take it down, as has occurred here, *see supra* n.4. The lack of any requirement for the covered person to certify that they have not themselves published the information that they are requesting not to be disclosed, or have made every effort to remove information that was self-published previously, further adds to the statute's under-inclusiveness.

be said to be a narrowly tailored means of safeguarding" the state's purported interests. *Schrader*, 74 F.4th at 127 (quoting *Fla. Star*, 491 U.S. at 538); *Sheehan*, 272 F. Supp. 2d at 1147 (finding that, having "inject[ed] personal identifying information into the public domain," the government "cannot credibly take the contradictory position" that other dissemination "offends a compelling state interest").[27]

Accordingly, the under-inclusiveness of Daniel's Law undermines any argument that the statute materially advances the state's purported interest, as required under the First Amendment.

3. The Legislature Has Less Restrictive Alternatives to Achieve Its Interest

This lack of tailoring in Daniel's Law is particularly "unacceptable" because the legislature ignored "less restrictive alternatives [that] would be at least as effective" in advancing its interest in enhancing public officials' safety. *Reno v. Am. Civ. Liberties Union*, 521 U.S. 844, 845–46 (1997). That is anathema to the First Amendment. "If a less restrictive alternative would serve the Government's purpose,

---

[27] Beyond exceptions to the statute that are specifically included in Daniel's Law itself, there may be other exceptions that arise by operation of other statutes. Indeed, at least one public agency has said that it likely cannot comply with Daniel's Law, because it is required by other laws to disclose certain information on campaign expenditures. New Jersey Election Law Enforcement Commission, 2023 Annual Report at 9 (April 2024), https://www.elec.nj.gov/pdffiles/annual_reports/annual2023.pdf, Ex. 31.

the legislature *must* use that alternative." *United States v. Playboy Entm't. Grp., Inc.*, 529 U.S. 803, 813 (2000) (emphasis added) (citation omitted).

The New Jersey legislature had, and continues to have, ample reasonable options to craft a more narrowly tailored statute aimed at enhancing the safety of public officials. Perhaps most saliently, it could enact a far more targeted prohibition than one that encompasses every type of "disclosure" imaginable, even where there has been no actual publication of the information at all. Further, the legislature could include—similar to what was in place before the 2023 amendments—a verification requirement for non-disclosure notices to private entities, to ensure that the individual is in fact a covered person. *See* N.J.S.A. 56:8-166.1(a)(1) (2021); *cf.* Cal. Gov't Code § 7928.215(c) (requiring non-disclosure demand to "include a statement describing a threat or fear for the safety" of the requesting official). The legislature could also include penalty provisions, if at all, that are based on fault—again, similar to what was in place before the 2023 amendments—and that do not create the potential for the statute to be used as an extortion instrument as Plaintiffs are seeking to use it here.[28]

[28] Defendants do not concede that these changes would be sufficient to render the statute constitutional. Rather, the point is that the Legislature was bound to consider these less restrictive alternatives and explain why they were insufficient.

"When plausible, less restrictive alternative[s] [are] offered to a content-based speech restriction, it is the Government's obligation to prove that the alternative [would] be ineffective to achieve its goals." *Playboy Entm't. Grp.*, 529 U.S. at 816. The legislature has not met that burden here. It has never attempted to explain why it did not pursue these obvious, less restrictive options. Nor has it explained why, in a series of amendments with no supporting legislative history, it has made the law consistently broader and harsher, and abandoned less speech-chilling alternatives that would effectively advance the state's interest.

Ultimately, the "Government's burden is not merely to show that a proposed less restrictive alternative has some flaws; its burden is to show that it is less effective." *Ashcroft v. ACLU*, 542 U.S. 656, 669 (2004) (citation omitted). In order to do so, the state "would have to show either that substantially less-restrictive alternatives were tried and failed, or that the alternatives were closely examined and ruled out for good reason." *Bruni*, 824 F.3d at 369-70 (reversing district court's dismissal of First Amendment challenge to buffer-zone ordinance where city did not show it considered less restrictive alternatives to achieving its interest). Absent a "meaningful" explanation as to why "alternative measures that burden substantially less speech would fail to achieve the government's interests"—an explanation that common sense suggests the legislature would never be able to furnish—Daniel's Law fails constitutional scrutiny. *Id.*

C. Daniel's Law Fails Even Intermediate Scrutiny

As explained above, Section IV.A, Daniel's Law is subject to strict scrutiny as a content-based restriction. But even if this Court somehow concludes that Daniel's Law is subject to intermediate scrutiny, the result should be the same. Intermediate scrutiny also has a heightened fit requirement that requires a speech restriction to be "narrowly drawn" to advance the state's "substantial" interest. *Cent. Hudson Gas & Elec. Corp.*, 447 U.S. at 565-66 . Like strict scrutiny, intermediate scrutiny demands that a speech restriction advance the stated interest "to a material degree." *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 505 (1996) (citation omitted). The existence of "less-burdensome alternatives" is also a crucial factor to consider in analyzing a speech restriction under intermediate scrutiny. *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 417 n.13 (1993).

Under this standard, "the 'fit' between the proposed restriction and the government's interest need not be the least restrictive means," but there still needs to be a "reasonable fit between the legislature's ends and the means chosen to accomplish those ends." *See Greater Phila. Chamber of Commerce v. City of Phila.*, 949 F.3d 116, 138 (3d Cir. 2020) (quoting *Lorillard Tobacco Co. v. Reilly*, 533 U.S. 525, 528 (2001)). That means that the government "may not regulate expression in such a manner that a substantial portion of the burden on speech does not serve to advance its goals." *McCullen*, 573 U.S. at 490 (citation omitted); *see Bd. of Trs. of*

State Univ. of N.Y. v. Fox, 492 U.S. 469, 479 (1989) (amount of speech prohibited under intermediate scrutiny may not be "substantially excessive" in relation to the state's purported interest).

For much the same reasons that Daniel's Law fails strict scrutiny, *see* Section IV.B, it easily fails intermediate scrutiny, too. Because of the tailoring problems detailed above, Daniel's Law prohibits far more speech than is necessary to achieve the state's interest, and its restrictions are not a "reasonable fit . . . narrowly tailored to achieve the desired objective" of enhancing public officials' safety. *Lorillard Tobacco Co.*, 533 U.S. at 561. And as explained at length above, the substantial under-inclusiveness of Daniel's Law prevents it from advancing the state's interest "to a material degree." *Liquormart*, 517 U.S. at 505 (citation omitted).

When, as here, speech restrictions are demonstrably over- or under-inclusive or leave significant holes in their coverage, courts do not hesitate to strike them down under intermediate scrutiny. In *Pitt News v. Pappert*, for example, the Third Circuit applied intermediate scrutiny to invalidate a statute prohibiting alcohol advertising to college students by media outlets affiliated with educational institutions, which was aimed at combatting underage alcohol consumption. 379 F.3d 96, 102 (3d Cir. 2004). The Court explained that the statute was "both severely over- and under-inclusive." *Id.* at 108. The statute was fatally over-inclusive because it also prevented certain communications with many adults "over the legal drinking age."

Id. And the statute was also under-inclusive—and so could not be said to advance the state's interest "to a material degree"— because minors would still be "exposed to a torrent" of "ads on television and the radio" and other forms of media. *Id.* at 107 (first citation omitted); *see also Rubin v. Coors Brewing Co.*, 514 U.S. 476, 488–89 (1995) (employing intermediate scrutiny to strike down under-inclusive statute); *Yim*, 63 F.4th at 795–96 (employing intermediate scrutiny to strike down over-inclusive statute).

The same considerations apply to Daniel's Law, given the substantial over-inclusiveness and under-inclusiveness of the statute, and the clear existence of less restrictive alternatives. *See supra* Part IV.B. Accordingly, even if this Court concludes that intermediate scrutiny applies, it should find the law unconstitutional.

D. Daniel's Law Is Unconstitutionally Vague

In addition to its other constitutional infirmities, Daniel's Law is also unconstitutionally vague. The law's provisions leave regulated parties unable to forecast what conduct could be punishable by harsh penalties and invite arbitrary enforcement.

A law is void for vagueness if it fails to provide sufficient notice of the conduct that is prohibited, such that "regulated parties [do not] know what is required of them," or is otherwise susceptible to arbitrary enforcement. *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253–54 (2012). Statutes must be written

clearly enough to "enable the ordinary citizen to conform his or her conduct to the law," as forcing parties to guess what conduct might be prohibited offends basic notions of fundamental fairness. *City of Chi. v. Morales*, 527 U.S. 41, 59 (1999). Requiring that a law provide "clear guidelines" to those responsible for enforcing it "ensure[s] fair and non-discriminatory application of the law[]." *N.J. Freedom Org. v. City of New Brunswick*, 7 F. Supp. 2d 499, 514–15 (D.N.J. 1997) (quoting *Kreimer v. Bureau of Police for Town of Morristown*, 958 F.2d 1242, 1266 (3d Cir. 1992)).

"When speech is involved," statutes must "rigorous[ly] adher[e]" to these requirements. *FCC*, 567 U.S. at 253–54. Vagueness in "content-based" speech regulations "raise[s] special First Amendment concerns because of [the] obvious chilling effect." *Reno*, 521 U.S. at 845–46. For this reason, courts apply "a more stringent" vagueness test to laws that restrict speech. *Franklin v. Navient Inc.*, 534 F. Supp. 3d 341, 347 (D. Del. 2021) (quoting *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.*, 455 U.S. 489, 499 (1982)).

Due to the sweeping breadth of its prohibition, Daniel's Law fails to provide sufficient notice of what is prohibited. As explained above, the statute's definition of "disclose" by itself encompasses a seemingly boundless range of conduct, potentially encompassing any type of "transfer" of a covered person's home address or phone number. N.J.S.A. 56:8-166.1(d). Again, the fact that the disclosure must occur "on the Internet," N.J.S.A. 56:8-166.1(a)(1), is not a significant limitation, as

the internet encompasses a vast variety of communications and data processing, not simply publishing content on a website. But making matters worse, the statutory prohibition does not stop with the phrase "disclose … on the Internet." It goes on to proscribe "otherwise mak[ing] available" a covered person's information—a completely undefined, open-ended phrase that, unlike "disclose," is not even modified by the phrase "on the Internet." N.J.S.A. 56:8-166.1(a)(1).

The statutory prohibition thus has no obvious limitation and leaves reasonable minds to guess at what conduct might be deemed to be barred by the statute. Someone in receipt of a non-disclosure notification made under the statute cannot be sure of all the things they need to do, or not do, to avoid potential liability. For example, is it permissible for a business to maintain a covered person's information in a file or database kept on a corporate share drive? The data is "available" to corporate employees in that circumstance. Is it permissible for a business to mail a letter or a package to the covered person at their home address? Or for Amazon to deliver a package? Putting the person's name and address on the envelope or the box could make it "available" to anyone in the mailroom or the warehouse. What about an employee writing the person's information on a post-it note and leaving it on their desk? It is "available" in that circumstance to anyone who walks by.

The poorly drawn terms of the statutory prohibition may cause businesses to refrain from *any* uses of a covered person's address or phone information, well

beyond any conduct that the legislature may have intended to prohibit—such as by purging the covered person's information from their records or refusing to do business with the person at all. Where a statute's ambiguities cause regulated parties to "steer far wider of the unlawful zone" by curtailing constitutionally protected conduct, its "vagueness cannot be tolerated." *Planned Parenthood of Cent. N.J. v. Verniero*, 41 F. Supp. 2d 478, 493–94 (D.N.J. 1998) (citations omitted).

The lack of definitional clarity also invites arbitrary—and abusive—enforcement. Countless businesses collect or use phone number or address information in one way or another, in the form of customer lists, account information, or otherwise, and often need that information to be "available" to various persons—such as employees, vendors, or business partners—as part of their everyday operations. Unbounded statutory terms mean that a litigation vehicle like Atlas has an endless set of businesses it can select as targets for abusive non-disclosure notifications and subsequent lawsuits like those brought here. That is precisely the sort of unpredictable enforcement that the void-for-vagueness doctrine exists to prevent. *See N.J. Freedom Org.*, 7 F. Supp. 2d at 515–16 (invalidating ordinance that would have required permit for any event of a certain size where money was solicited, because its breadth rendered it susceptible to selective enforcement); *cf. Bd. of Airport Comm'rs v. Jews for Jesus, Inc.*, 482 U.S. 569, 576 (1987) (law that potentially captured all speech in airport terminal violated First Amendment because

"[t]he opportunity for abuse, especially where a statute has received a virtually open-ended interpretation, is self-evident" (citation omitted)).

Likewise, the requirement that businesses take down "*unpublished* home telephone numbers" of covered persons, N.J.S.A. 56:8-166.1(a) (emphasis added), provides insufficient notice of the conduct prohibited by the statute. The statute provides no definition of what it means for a home telephone number to be "unpublished." And, in this day and age, no standard exists to distinguish "published" telephone numbers from "unpublished" numbers: The terms are an anachronism tied to local telephone directories, which are largely a thing of the past. Accordingly, the recipient of a non-disclosure request under Daniel's Law has no way to determine whether a telephone number is "unpublished"—and therefore subject to the statute—or "published"—and therefore not. This provision is therefore also unconstitutionally vague.

V. CONCLUSION

For these reasons, Daniel's Law violates the First Amendment and the Free Speech Clause of the New Jersey State Constitution, and is unconstitutionally vague. This Court should therefore grant Defendants' motion and dismiss Plaintiffs' claims with prejudice.

Dated: June 10, 2024

LATHAM & WATKINS LLP

/s/ *Kevin M. McDonough*

Kevin M. McDonough (ID: 41892005)
Serrin Turner (*pro hac vice*)
LATHAM & WATKINS LLP
1271 Avenue of Americas
New York, NY 10020
Telephone: (212) 906-1200
Email: kevin.mcdonough@lw.com
serrin.turner@lw.com

Bradley M. Baglien (*pro hac vice*)
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, D.C. 20004-1304
Telephone: (202) 637-2200
Email: bradley.baglien@lw.com

Attorneys for Defendants LightBox Parent, L.P. and LightBox Holdings, L.P.

Dated: June 10, 2024

CARLTON FIELDS

/s/ *Michael T. Hensley*
Michael T. Hensley
Jorkeell Echeverria
180 Park Avenue, Suite 106
Florham Park, New Jersey 07932
Tel: 973.828.2613
Fax: 212.430.5501
MHensley@carltonfields.com
JEcheverria@carltonfields.com

PARKER POE ADAMS & BERNSTEIN LLP

Sarah F. Hutchins (*pro hac vice*)
Corri A. Hopkins (*pro hac vice*)
620 South Tryon Street, Suite 800
Charlotte, North Carolina 28202
Tel: 704.335.6639
sarahhutchins@parkerpoe.com
corrihopkins@parkerpoe.com

Attorneys for Defendant Blackbaud, Inc.

Dated: June 10, 2024

VEDDER PRICE P.C.

/s/ *Blaine C. Kimrey*
Blaine C. Kimrey (*pro hac vice*)
bkimrey@vedderprice.com
Bryan K. Clark (*pro hac vice*)
bclark@vedderprice.com
222 N. LaSalle Street
Chicago, IL 60601
T: +1 312 609 7500
F: +1 312 407 5005

Jean A. Occhiogrosso
jocchiogrosso@vedderprice.com

Vedder Price P.C.
1633 Broadway, 31st Floor
New York, New York 10019
T: +1 212 407 7700
F: +1 212 407 7799

Attorneys for Defendant Whitepages, Inc.

Dated: June 10, 2024

VEDDER PRICE P.C.

/s/ *Blaine C . Kimrey*
Blaine C. Kimrey (*pro hac vice*)
bkimrey@vedderprice.com
Bryan K. Clark (*pro hac vice*)
bclark@vedderprice.com
222 N. LaSalle Street
Chicago, IL 60601
T: +1 312 609 7500
F: +1 312 407 5005

Jean A. Occhiogrosso
jocchiogrosso@vedderprice.com
Vedder Price P.C.
1633 Broadway, 31st Floor
New York, New York 10019
T: +1 212 407 7700
F: +1 212 407 7799

Attorneys for Defendant Hiya, Inc.

Dated: June 10, 2024

SEYFARTH SHAW LLP

/s/ *Robert T. Syzba*
Robert T. Szyba
SEYFARTH SHAW LLP
620 Eighth Avenue, 32nd Floor
New York, NY 10018-1405
Telephone: (212) 218-5500
Email: rszyba@seyfarth.com

Attorneys for Defendant We Inform, LLC

Dated: June 10, 2024

SEYFARTH SHAW LLP

/s/ *Robert T. Syzba*
Robert T. Szyba
SEYFARTH SHAW LLP
620 Eighth Avenue, 32nd Floor
New York, NY 10018-1405
Telephone: (212) 218-5500
Email: rszyba@seyfarth.com

Attorneys for Defendant Infomatics, LLC

Dated: June 10, 2024

SEYFARTH SHAW LLP

/s/ *Robert T. Syzba*
Robert T. Szyba
SEYFARTH SHAW LLP
620 Eighth Avenue, 32nd Floor
New York, NY 10018-1405
Telephone: (212) 218-5500
Email: rszyba@seyfarth.com

Attorneys for Defendant The People Searchers, LLC

Dated: June 10, 2024

DENTONS US LLP

/s/ *Stephen M. Turner*
Stephen M. Turner, Esq.
DENTONS US LLP
101 JFK Parkway, 4th Floor
Short Hills, NJ 07078
Telephone: (973) 912-7146
Email: stephen.turner@dentons.com

Bety Javidzad, Esq. (*pro hac vice*)
DENTONS US LLP
601 South Figueroa Street, Suite 2500
Los Angeles, CA 90017
Telephone: (213) 243-6115
Email: bety.javidzad@dentons.com

Attorneys for Defendant Commercial Real Estate Exchange, Inc.

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ Angelo A. Stio III
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant DM Group.Inc.

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ Angelo A. Stio III
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227

Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant Carco Group Inc.

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ Angelo A. Stio III
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant Deluxe Corp.

Dated: June 10, 2024

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Camille Joanne Rosca
Camille Joanne Rosca
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019-6142
Telephone: +1 212 506 5000
Email: crosca@orrick.com

Attorneys for Defendant
TWILIO INC.

Dated: June 10, 2024

SPIRO HARRISON & NELSON

/s/ Thomas M. Kenny
Thomas M. Kenny, Esq.
Francesca Simone, Esq.
363 Bloomfield Avenue, Suite 2C
Montclair, NJ 07042

Attorneys for Defendants Quantarium Alliance, LLC and Quantarium Group, LLC

Dated: June 10, 2024

QUINN EMANUEL URQUHART & SULLIVAN, LLP

/s/ Anthony J. Staltari
Anthony J. Staltari (ID No. 233022017)
51 Madison Avenue, 22nd Floor
New York, New York 10010
Tel.: (212) 849-7000
Email: anthonystaltari@quinnemanuel.com

Viola Trebicka (*pro hac vice*)
John Wall Baumann (*pro hac vice*)
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
violatrebicka@quinnemanuel.com
jackbaumann@quinnemanuel.com

Ella Hallwass (*pro hac vice*)
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
ellahallwass@quinnemanuel.com

Xi ("Tracy") Gao (*pro hac vice*)
1300 I Street NW, Suite 900
Washington D.C., 20005
Telephone: (202) 538-8000
tracygao@quinnemanuel.com

Attorneys for Defendant Yardi Systems, Inc.

Dated: June 10, 2024

CLARK HILL PLC

/s/ Myriah V. Jaworski
Myriah V. Jaworski (*pro hac vice*)
Chirag H. Patel (*pro hac vice*)
Steven Richman, Esq.
210 Carnegie Center, Suite 102
Princeton, NJ 08540
(609) 785-2911
Email: mjaworski@clarkhill.com
cpatel@clarkhill.com
srichman@clarkhill.com

Attorneys for Defendant 6sense Insights, Inc.

Dated: June 10, 2024

CLARK HILL PLC

/s/ Myriah V. Jaworski
Myriah V. Jaworski (*pro hac vice*)
Chirag H. Patel (*pro hac vice*)
Steven Richman, Esq.
210 Carnegie Center, Suite 102
Princeton, NJ 08540
(609) 785-2911
Email: mjaworski@clarkhill.com
cpatel@clarkhill.com
srichman@clarkhill.com

Attorneys for Defendant

Search Quarry LLC

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ Angelo A. Stio III
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant Acxiom LLC

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ Angelo A. Stio III
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendants Enformion, LLC and Enformion Holdco, Inc.

Dated: June 10, 2024

LATHAM & WATKINS LLP

/s/ *Kevin M. McDonough*
Kevin M. McDonough (ID: 41892005)
Serrin Turner (*pro hac vice*)
LATHAM & WATKINS LLP
1271 Avenue of Americas
New York, NY 10020
Telephone: (212) 906-1200
Email: kevin.mcdonough@lw.com
serrin.turner@lw.com

Bradley M. Baglien (*pro hac vice*)
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, D.C. 20004-1304
Telephone: (202) 637-2200
Email: bradley.baglien@lw.com

Attorneys for Defendants CoStar Group, Inc. and CoStar Realty Information, Inc.

Dated: June 10, 2024

LATHAM & WATKINS LLP

/s/ *Kevin M. McDonough*
Kevin M. McDonough (ID: 41892005)
Serrin Turner (*pro hac vice*)
LATHAM & WATKINS LLP
1271 Avenue of Americas
New York, NY 10020
Telephone: (212) 906-1200
Email: kevin.mcdonough@lw.com
serrin.turner@lw.com

Jennifer C. Archie (*pro hac vice*)
Bradley M. Baglien (*pro hac vice*)

LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, D.C. 20004-1304
Telephone: (202) 637-2200
Email: jennifer.archie@lw.com
bradley.baglien@lw.com

Robert C. Collins (*pro hac vice*)
LATHAM & WATKINS LLP
330 N. Wabash Ave, Suite 2800
Chicago, IL 60611
Telephone: (312) 876-7700
Email: robert.collins@lw.com

Attorneys for Defendants Oracle International Corporation, Oracle America, Incorporated, and Oracle Corporation

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ Angelo A. Stio III

Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant Red Violet, Inc.

Dated: June 10, 2024

KELLEY DRYE & WARREN LLP

/s/ Lauri A. Mazzuchetti
Lauri A. Mazzuchetti
Whitney M. Smith
Aaron J. Gold
KELLEY DRYE & WARREN LLC
One Jefferson Road, 2nd Floor
Parsippany, NJ 07054
Tel: (973) 503-5900
Fax: (973) 503-5950
lmazzuchetti@kelleydrye.com
wsmith@kelleydrye.com
agold@kelleydrye.com

Counsel for Defendant
RE/MAX, LLC

Dated: June 10, 2024

FAEGRE DRINKER BIDDLE & REATH LLP

/s/ Ross A. Lewin
Ross A. Lewin
Faegre Drinker Biddle & Reath LLP
105 College Road East
Princeton, New Jersey 08542

Kevin DeMaio
600 Campus Drive
Florham Park, New Jersey 07932
ross.lewin@faegredrinker.com
kevin.demaio@faegredrinker.com

HARRISON LAW LLC
Rachel B. Niewoehner *(pro hac vice)*
Katherine A.G. Sobiech *(pro hac vice)*
141 West Jackson Boulevard,
Suite 2055
Chicago, Illinois 60604
(312) 638-8776

Attorneys for Defendants
Epsilon Data Management, LLC,
Conversant LLC, and
Citrus Ad International, Inc.

Dated: June 10, 2024

STARR, GERN, DAVISON & RUBIN, P.C.

/s/ Richard T. Welch
Richard T. Welch, Esq. (032982006)
Ronald L. Davison, Esq. (266481971)
Starr, Gern, Davison & Rubin, P.C.
105 Eisenhower Parkway, Suite 401
Roseland, NJ 07068-1640
Tel: 973.403.9200
rwelch@starrgern.com
rdavison@starrgern.com

ZWILLGEN PLLC

Jacob Sommer, Esq.
1900 M. Street NW, Suite 250
Washington, DC 20036
Tel: 202.706.5205
jake@zwillgen.com
(Admitted Pro Hac Vice)

Sudhir Rao, Esq.
183 Madison Avenue, Suite 1504
New York, NY 10016

Tel: 646.362.5590
Sudhir.Rao@zwillgen.com
(Admitted Pro Hac Vice)

Attorneys for Defendant People Data Labs, Inc.

Dated: June 10, 2024

STOEL RIVES LLP

/s/ Misha Isaak

Misha Isaak
misha.isaak@stoel.com
James A. Kilcup
james.kilcup@stoel.com
Alexandra Choi Giza
alexandra.giza@stoel.com
STOEL RIVES LLP
760 SW Ninth Ave, Suite 3000
Portland, OR 97205
Telephone: (503) 224-3380

Ryan J. Cooper
ryan@cooperllc.com
COOPER, LLC
108 N. Union Ave., Suite 4
Cranford, NJ 07016
Telephone: (908) 514-8830

Counsel for Defendant Labels & Lists, Inc.

Dated: June 10, 2024

GORDON, REES, SCULLY & MANSUKHANI LLP

/s/ Douglas Motzenbecker

Douglas Motzenbecker, Esq.
Joseph Salvo, Esq. (*pro hac vice forthcoming*)
John Mills, Esq. (*pro hac vice forthcoming*)

Bianca Evans, Esq. (pro hac vice)
1 Battery Park Plaza
Suite 2801
New York, NY 10004
Telephone: (212) 453-0725
Facsimile: (212) 269-5505
dmotzenbecker@grsm.com
jsalvo@grsm.com
jtmills@grsm.com
bevans@grsm.com

Attorneys for Defendant Claritas LLC

Dated: June 10, 2024

PIERSON FERDINAND LLP

/s/ Jill A, Guldin
Jill A. Guldin, Esq. (No. 93657)
One Liberty Place
1650 Market Street, 36th Floor
Philadelphia, PA 19103
Telephone: (856) 896-4096
Facsimile: (856) 494-1566
Email: jill.guldin@pierferd.com

FISHERBROYLES, LLP
Jason A. Spak (*admitted pro hac vice*)
6360 Broad Street #5262
Pittsburgh, PA 15206
T: 412-230-8555
F: 412-774-2382
E: jason.spak@fisherbroyles.com

Counsel for Defendant Innovis Data Solutions, Inc.

Dated: June 10, 2024

CONSTANGY BROOKS, SMITH & PROHPHET LLP

/s/ John E. MacDonald
John E. MacDonald (011511995)
Princeton South Corporate Center
3120 Princeton Pike, Suite 301
Lawrenceville, NJ 08648
Phone: (609) 357-1183
Fax: (609) 844-1102
jmacdonald@constangy.com

Attorneys for Defendant Accurate Append, Inc.

Dated: June 10, 2024

TRESSLER LLP

/s/ Timothy M.. Jabbour
Timothy M. Jabbour (ID:TJ5611)
George Z. Twill (ID: 275292018)
Tressler LLP
163 Madison Avenue, Suite 404
Morristown, NJ 07960
973-848-2901
tjabbour@tresslerllp.com
gtwill@tresslerllp.com

Gregory C. Scaglione (pro hac vice)
Timothy Hutchinson (pro hac vice)
Koley Jessen P.C., L.L.O.
1125 S. 103rd St., Suite 800
Omaha, NE 68124
531-444-0644
Greg.Scaglione@koleyjessen.com
Tim.Hutchinson@koleyjessen.com

Attorneys for Defendant Data Axle, Inc.

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ Angelo A. Stio III
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant Remine Inc.

Dated: June 10, 2024

GORDON, REES, SCULLY & MANSUKHANI LLP

/s/ Douglas Motzenbecker
Douglas Motzenbecker, Esq.
Joseph Salvo, Esq. (*pro hac vice forthcoming*)
John Mills, Esq. (*pro hac vice forthcoming*)

Bianca Evans, Esq. (pro hac vice)
1 Battery Park Plaza
Suite 2801
New York, NY 10004
Telephone: (212) 453-0725
Facsimile: (212) 269-5505
dmotzenbecker@grsm.com
jsalvo@grsm.com
jtmills@grsm.com
bevans@grsm.com

Attorneys for Defendant Lusha Systems Inc.

Dated: June 10, 2024

CARLTON FIELDS, P.A.

/s/ Douglas Motzenbecker

Michael D. Margulies (No. 030412008)
CARLTON FIELDS, P.A.
180 Park Avenue, Suite 106
Florham Park, NJ 07932
Telephone: (973) 828-2600
Email: mmargulies@carltonfields.com

Attorneys for Defendant Teltech Systems, Inc.

Dated: June 10, 2024

LATHAM & WATKINS LLP

/s/ *Kevin M. McDonough*

Kevin M. McDonough (ID: 41892005)
LATHAM & WATKINS LLP
1271 Avenue of Americas
New York, NY 10020
Telephone: (212) 906-1200
Email: kevin.mcdonough@lw.com

Jennifer C. Archie (*pro hac vice*)
Bradley M. Baglien (*pro hac vice*)
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, D.C. 20004-1304
Telephone: (202) 637-2200
Email: jennifer.archie@lw.com
bradley.baglien@lw.com

Robert C. Collins (*pro hac vice*)

LATHAM & WATKINS LLP
330 N. Wabash Ave, Suite 2800
Chicago, IL 60611
Telephone: (312) 876-7700
Email: robert.collins@lw.com

Attorneys for Defendants PeopleConnect, Inc., PeopleConnect Holdings, Inc., Intelius, LLC, and PeopleConnect Intermediate, LLC

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ Angelo A. Stio III

Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant Corelogic, Inc.

Dated: June 10, 2024

McCARTER & ENGLISH, LLP

/s/ Scott S. Christie

Scott S. Christie (ID: 37901989)
Four Gateway Center
100 Mulberry Street
Newark, NJ 07102
Telephone: (973) 622-4444
Email: schristie@mccarter.com

Curtis B. Leitner
McCARTER & ENGLISH, LLP
Worldwide Plaza
825 Eighth Ave., 31st Floor
New York, NY 10019
Telephone: (212) 609-6800
Email: cleitner@mccarter.com

Attorneys for Defendants Defendants Black Knight Technologies, LLC and Black Knight, Inc.

Dated: June 10, 2024

BUCHANAN INGERSOLL & ROONEY P.C.

/s/ Samantha L. Southall

Samantha L. Southall (admitted pro hac vice)
Two Liberty Place
50 S. 16th Street, Suite 3200
Philadelphia, PA 19102-2555
215 665 3884 (o)
samantha.southall@bipc.com

Jacqueline M. Weyand
550 Broad Street, Suite 810
Newark, New Jersey 07102
973 273 9800 (o)
jacqueline.weyand@bipc.com

Attorneys for Defendant Zillow, Inc.

Dated: June 10, 2024

GIBBONS P.C.

/s/ Frederick W. Alworth
Frederick W. Alworth
Kevin R. Reich
GIBBONS P.C.
One Gateway Center
Newark, New Jersey 07102-5310
Tel: (973) 596-4500
falworth@gibbonslaw.com
kreich@gibbonslaw.com

Attorneys for Defendant Equimine, Inc.

Dated: June 10, 2024

BALLARD SPAHR LLP

/s/ Marcel S. Pratt
Marcel S. Pratt
Michael Berry (appearance forthcoming)
John W. Scott
Jordan Meyer
1735 Market Street, Fl. 51
Philadelphia, PA 19103-7599
215.864.8605
prattm@ballardspahr.com
berrym@ballardspahr.com
scottj@ballardspahr.com
meyerjl@ballardspahr.com

Attorneys for Defendants Thomson Reuters Corporation, Thomson Reuters Holdings Inc., Thomson Reuters Canada Limited, and Thomson Reuters Applications Inc.

Dated: June 10, 2024

BALLARD SPAHR LLP

/s/ Alan Schoenfeld
Alan Schoenfeld (New Jersey Bar No. 285532018)
Marissa M. Wenzel (*pro hac vice*)
Todd Clayton (*pro hac vice*)
WILMER CUTLER PICKERING
HALE AND DORR LLP
7 World Trade Center
250 Greenwich Street
New York, NY 10007
(212) 230-8800 (phone)
(212) 230-8888 (fax)
alan.schoenfeld@wilmerhale.com
marissa.wenzel@wilmerhale.com
todd.clayton@wilmerhale.com

Christopher Davies (*pro hac vice*)
WILMER CUTLER PICKERING
HALE AND DORR LLP
2100 Pennsylvania Avenue NW
Washington, DC 20037
(202) 663-6000 (phone)
(202) 663-6363 (fax)
christopher.davies@wilmerhale.com

Attorneys for Defendant Choreograph LLC

Dated: June 10, 2024

BUCHANAN INGERSOLL & ROONEY P.C.

/s/ Samantha L. Southall
Samantha L. Southall (admitted pro hac vice)
Two Liberty Place
50 S. 16th Street, Suite 3200
Philadelphia, PA 19102-2555
215 665 3884 (o)

samantha.southall@bipc.com

Jacqueline M. Weyand
550 Broad Street, Suite 810
Newark, New Jersey 07102
973 273 9800 (o)
jacqueline.weyand@bipc.com

Attorneys for Defendant Transunion LLC

Dated: June 10, 2024

RIKER DANZIG LLP

/s/ *Michael P. O'Mullan*
Michael P. O'Mullan (ID 029681996)
Headquarters Plaza
One Speedwell Avenue
Morristown, NJ 07962
Telephone: (973) 451-8477
Email: momullan@riker.com

Attorneys for Defendant Melissa Data Corporation

Dated: June 10, 2024

KING & SPALDING LLP

/s/ Thomas J. Scrivo
Thomas J. Scrivo
King & Spalding LLP
1185 Avenue of the Americas
34th Floor
New York, NY 10036-2601
Tel: 212-556-2100
Fax: 212-556-2222
Email: tscrivo@kslaw.com

Zachary A. McEntyre*
John C. Toro*
Charles G. Spalding, Jr.**
King & Spalding LLP

1180 Peachtree Street
Atlanta, GA 30309
Tel.: (404) 572-4600
Fax: (404) 572-5100
Email: zmcentyre@kslaw.com
Email: jtoro@kslaw.com
Email: cspalding@kslaw.com

*Admitted Pro Hac Vice
**Pro Hac Vice forthcoming

Counsel for Equifax Inc. and Kount Inc.

Dated: June 10, 2024

SILLS CUMMIS & GROSS P.C.

/s/ *Joshua N. Howley*
Joshua N. Howley
SILLS CUMMIS & GROSS P.C.
One Riverfront Plaza
Newark, NJ 07102
(973) 643-7000
jhowley@sillscummis.com

Andrew J. Pincus*
MAYER BROWN LLP
1999 K Street NW
Washington, DC 20006
(202) 263-3000
apincus@mayerbrown.com

John Nadolenco
Daniel D. Queen
MAYER BROWN LLP
333 S. Grand Avenue
Los Angeles, CA 90071
(213) 229-9500
jnadolenco@mayerbrown.com

Benjamin D. Bright*
Jonathan D. Stahl*
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
(212) 506-2500
bbright@mayerbrown.com

*pro hac vice

Attorneys for Defendant Spokeo, Inc.

Dated: June 10, 2024

STINSON LLP

/s/ *Richard J.L. Lomuscio*
Richard J.L. Lomuscio
100 Wall Street, Suite 201
New York, New York 10005
Telephone: 646-883-7471
richard.lomuscio@stinson.com

Matthew D. Moderson
1201 Walnut Street, Suite 2900
Kansas City, Missouri 64106
Telephone: 816-691-2736
matt.moderson@stinson.com

Attorneys for i360, LLC

Dated: June 10, 2024

McCARTER & ENGLISH, LLP

/s/ *Scott S. Christie* .
Scott S. Christie (ID: 37901989)
Four Gateway Center
100 Mulberry Street
Newark, NJ 07102
Telephone: (973) 622-4444
Email: schristie@mccarter.com

Attorneys for Defendant Telnyx LLC

Dated: June 10, 2024

GREENBERG TRAURIG, LLP

/s/ *Arron Van. Nostrand .*
Aaron Van Nostrand
GREENBERG TRAURIG, LLP
500 Campus Drive, Suite 400
Florham Park, NJ 07932-0677
(973) 360-7900

Attorneys for Defendant
Gohunt LLC

Dated: June 10, 2024

LOWENSTEIN SANDLER LLP

/s/ *Jennifer Fiorica Delgado.*
Jennifer Fiorica Delgado
Markiana J. Julceus
One Lowenstein Drive
Roseland, New Jersey 07068
646.414.6962
862.926.2707
jdelgado@lowenstein.com
mjulceus@lowenstein.com

Attorneys for Defendant AccuZIP, Inc.

Dated: June 10, 2024

LEWIS BRISBOIS BISGAARD & SMITH, LLP

/s/ *Thomas C. Regan.*
Thomas C. Regan, Esq.
Matthew S. AhKao, Esq.
LEWIS BRISBOIS BISGAARD & SMITH, LLP
One Riverfront Plaza, Suite 800
Newark, NJ 07102
Telephone: (973) 577-6260

Email:
Thomas.Regan@lewisbrisbois.com
Matthew.AhKao@lewisbrisbois.com

Attorneys for Defendant Synaptix Technology, LLC

Dated: June 10, 2024

GREENSPOON MARDER

/s/ *Kelly M. Purcaro.*

Kelly M. Purcaro, Esq. (ID: 017692009)
Kory Ann Ferro, Esq. (ID: 065932013)
GREENSPOON MARDER
One Riverfront Plaza
1037 Raymond Blvd., Suite 900
Newark, New Jersey 07102
Tel.: (732) 456-8746
Kelly.Purcaro@gmlaw.com
KoryAnn.Ferro@gmlaw.com

Attorneys for Defendants Joy Rockwell Enterprises, Inc. d/b/a PostcardMania PCM LLC

Dated: June 10, 2024

THOMPSON HINE LLP

/s/ J. Timothy McDonald

J. Timothy McDonald (ID No. 027201990)
Jennifer A. Adler (pro hac vice)
THOMPSON HINE LLP
Two Alliance Center
3560 Lenox Road, Suite 1600
Atlanta, Georgia 30326
Phone: 404.541.2900
Fax: 404.541.2906
Tim.McDonald@thompsonhine.com
Jennifer.Adler@thompsonhine.com

Steven G. Stransky (*pro hac vice*)
THOMPSON HINE LLP
3900 Key Center
127 Public Square
Cleveland, Ohio 44114
Phone: 216.566.5500
Fax: 216.566.5800
Steve.Stransky@thompsonhine.com

Attorneys for Defendant Fortnoff Financial, LLC

Dated: June 10, 2024

MCELROY, DEUTSCH, MULVANEY, & CARPENTER, LLP

/s/ *Nicholas K. Lagemann*

Nicholas K. Lagemann
MCELROY, DEUTSCH,
MULVANEY, & CARPENTER, LLP
1300 Mount Kemble Avenue
Morristown, NJ 07962
Tel: (973) 425-8210
NLagemann@mdmc-law.com

Jacquelyn Fradette (*pro hac vice*)
Alan Charles Raul (*pro hac vice*)
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, D.C. 20005
(202) 736-8822
jfradette@sidley.com
araul@sidley.com

Tyler J. Domino (*pro hac vice*)
SIDLEY AUSTIN LLP
787 Seventh Avenue
New York, NY 10019
(212) 839-5300

tdomino@sidley.com

Attorneys for Defendants MyHeritage Ltd. and MyHeritage (USA), Inc.

Dated: June 10, 2024

RKW, LLC

/s/ *Stacy Torres* .
H. Mark Stichel*
Stacey Torres (293522020)
10075 Red Run Blvd, Ste 401
Owings Mills, Maryland 21117
(443) 379-8941
storres@rkwlawgroup.com

*Admitted pro hac vice

Attorneys for Defendant eMerges.com Inc.

Dated: June 10, 2024

DENTONS US LLP

/s/ *Stephen M. Turner*
Stephen M. Turner, Esq.
DENTONS US LLP
101 JFK Parkway, 4th Floor
Short Hills, NJ 07078
Telephone: (973) 912-7146
Email: stephen.turner@dentons.com

Kristen C. Rodriguez, Esq. (admitted pro hac vice)
DENTONS US LLP
1221 Avenue of the Americas
New York, NY 10020
Telephone: (212) 398-5280
Email:
kristen.rodriguez@dentons.com

Attorneys for Defendant Wiland, Inc.

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ *Angelo A. Stio*
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant AtData LLC.

Dated: June 10, 2024

SAUL EWING LLP

/s/ *William C. Baton*
William C. Baton
Sarah A. Sullivan
Alexander L. Callo
SAUL EWING LLP
One Riverfront Plaza
1037 Raymond Blvd.
Newark, NJ 07102-5426
(973) 286-6700
wbaton@saul.com
sarah.sullivan@saul.com

COOLEY LLP
Matthew D. Brown (admitted pro hac vice)
Bethany C. Lobo (admitted pro hac vice)
3 Embarcadero Center, 20th Floor
San Francisco, CA 94111
Telephone: (415) 693-2000

E-mail: brownmd@cooley.com
E-mail: blobo@cooley.com

Rebecca L. Tarneja (admitted pro hac vice)
355 S. Grand Avenue, Suite 900
Los Angeles, CA 90071
Telephone: (213) 561-3250
E-mail: rtarneja@cooley.com

Attorneys for Defendants Precisely Holdings, LLC, Precisely Software Inc., and Precisely Software Ltd.

Dated: June 10, 2024

GORDON REES SCULLY MANSUKHANI LLP

/s/ *Clair E. Wischusen*
Clair E. Wischusen (ID: 018022009)
Bianca C. Evans (pro hac vice)
18 Columbia Turnpike
Suite 220
Florham Park, NJ 07932
Telephone: (973) 549-2500
Email: cwischusen@grsm.com
bevans@grsm.com

Attorneys for Defendant, Nuwber, Inc.

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ *Angelo A. Stio*
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227

Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant Rocketreach LLC

Dated: June 10, 2024

GREENBERG TRAURIG, LLP

/s/ *Arron Van. Nostrand* .

Aaron Van Nostrand
GREENBERG TRAURIG, LLP
500 Campus Drive, Suite 400
Florham Park, NJ 07932-0677
(973) 360-7900

Attorneys for Defendant Outside Interactive, Inc.

Dated: June 10, 2024

SAUL EWING LLP

/s/ *William C. Baton*

William C. Baton
Sarah A. Sullivan
Alexander L. Callo
SAUL EWING LLP
One Riverfront Plaza
1037 Raymond Blvd.
Newark, NJ 07102-5426
(973) 286-6700
wbaton@saul.com
sarah.sullivan@saul.com
alexander.callo@saul.com

COOLEY LLP
Matthew D. Brown (admitted pro hac vice)
Bethany C. Lobo (admitted pro hac vice)
3 Embarcadero Center, 20th Floor

San Francisco, CA 94111
Telephone: (415) 693-2000
E-mail: brownmd@cooley.com
E-mail: blobo@cooley.com

Rebecca L. Tarneja (admitted pro hac vice)
355 S. Grand Avenue, Suite 900
Los Angeles, CA 90071
Telephone: (213) 561-3250
E-mail: rtarneja@cooley.com

Attorneys for Defendants Valassis Digital Corp. and Valassis Communications, Inc.

Dated: June 10, 2024

MANATT, PHELPS & PHILLIPS, LLP

/s/ *Kenneth D. Friedman*

Kenneth D. Friedman
7 Times Square
New York, New York 10036
(212) 790-4500
kfriedman@manatt.com

Kareem A. Salem (pro hac vice)
Brandon Reilly (pro hac vice)
662 Encinitas Blvd., Suite 216
Encinitas, CA 92024
(619) 205-8520
ksalem@manatt.com
breilly@manatt.com

Attorneys for Defendant Vericast Corp.

Dated: June 10, 2024

MCCARTER & ENGLISH LLP

/s/ *Christopher A. Rojao*
Ryan A. Savercool
Four Gateway Center
100 Mulberry Street
Newark, New Jersey 07102
(973) 622-4444
crojao@mccarter.com
rsavercool@mccarter.com

HOGAN LOVELLS US LLP
/s/ Jon M. Talotta
Jon M. Talotta (admitted pro hac vice)
8350 Broad Street (Boro Tower)
Tysons, VA 22102
Tel: 703.610.6100
jon.talotta@hoganlovells.com
David M. Cheifetz (admitted pro hac vice)
Elizabeth C. Milburn (pro hac vice to be filed)
390 Madison Avenue
New York, New York 10017
Tel: 212.918.3000
david.cheifetz@hoganlovells.com
tina.milburn@hoganlovells.com

Attorneys for Defendants in 1:24-cv-4850-HB, The Lifetime Value Co. LLC, BeenVerified, LLC, NeighborWho LLC, The NumberGuru, LLC, PeopleLooker LLC, PeopleSmart LLC, Ownerly, LLC

Dated: June 10, 2024

BLANK ROME

/s/ *Phillip N. Yannella*____
STEPHEN M. ORLOFSKY
NEW JERSEY RESIDENT
PARTNER
PHILIP N. YANNELLA
GREGORY A. BAILEY
300 Carnegie Center, Suite 220
Princeton, NJ 08540
Telephone: (609) 750-7700
Facsimile: (609) 750-7701
Stephen.Orlofsky@BlankRome.com
Philip.Yannella@BlankRome.com
Gregory.Bailey@BlankRome.com

Attorneys for Defendant
Belles Camp Communications, Inc.

Dated: June 10, 2024

MONTGOMERY MCCRACKEN WALKER & RHOADS LLP

/s/ *Alexandra S. Jacobs*____
Alexandra S. Jacobs
John Papianou
457 Haddonfield Road, Suite 600
Cherry Hill, NJ 08002
856.488.7746
ajacobs@mmwr.com
jpapianou@mmwr.com

HUDSON COOK LLP
Rebecca E. Kuehn (pro hac vice forthcoming)
Robert D. Tilley (pro hac vice forthcoming)
Jason F. Esteves (pro hac vice forthcoming)
1909 K Street, NW, 4th Floor
Washington, DC 20006

202.327.9710 / 202.327.9711
rkuehn@hudco.com
rtilley@hudco.com
jesteves@hudco.com

Attorneys for Defendant, First American Financial Corporation

Dated: June 10, 2024

TROUTMAN PEPPTER HAMILTON SANDER LLP

/s/ *Angelo A. Stio*
Angelo A. Stio III
Melissa A. Chuderewicz
TROUTMAN PEPPER HAMILTON SANDERS LLP
Suite 400
301 Carnegie Center
Princeton, NJ 08540-6227
Telephone: (609) 951-4125
Email: angelo.stio@troutman.com
melissa.chuderwicz@troutman.com

Attorneys for Defendant Property Radar, Inc.

Dated: June 10, 2024

GREENSPOON MARDER

/s/ *Kelly M. Purcaro.*
Kelly M. Purcaro, Esq. (ID: 017692009)
Kory Ann Ferro, Esq. (ID: 065932013)
GREENSPOON MARDER
One Riverfront Plaza
1037 Raymond Blvd., Suite 900
Newark, New Jersey 07102
Tel.: (732) 456-8746
Kelly.Purcaro@gmlaw.com
KoryAnn.Ferro@gmlaw.com

Attorneys for Defendants
The Alesco Group, LLC

Dated: June 10, 2024

GREENSPOON MARDER

/s/ *Kelly M. Purcaro*
Kelly M. Purcaro, Esq. (ID: 017692009)
Kory Ann Ferro, Esq. (ID: 065932013)
GREENSPOON MARDER
One Riverfront Plaza
1037 Raymond Blvd., Suite 900
Newark, New Jersey 07102
Tel.: (732) 456-8746
Kelly.Purcaro@gmlaw.com
KoryAnn.Ferro@gmlaw.com

Attorneys for Defendants
Searchbug, Inc.

Dated: June 10, 2024

GREENSPOON MARDER

/s/ *Kelly M. Purcaro.*
Kelly M. Purcaro, Esq. (ID: 017692009)
Kory Ann Ferro, Esq. (ID: 065932013)
GREENSPOON MARDER
One Riverfront Plaza
1037 Raymond Blvd., Suite 900
Newark, New Jersey 07102
Tel.: (732) 456-8746
Kelly.Purcaro@gmlaw.com
KoryAnn.Ferro@gmlaw.com

Attorneys for Defendants
Amerilist, Inc.

Dated: June 10, 2024

LOWENSTEIN SANDLER LLP

/s/ A. Matthew Boxer

A. Matthew Boxer
Gavin J. Rooney
Rasmeet K. Chahil
LOWENSTEIN SANDLER LLP
One Lowenstein Drive
Roseland, New Jersey 07068
973.597.2500
mboxer@lowenstein.com
grooney@lowenstein.com
rchahil@lowenstein.com

Attorneys for Defendants LexisNexis Risk Data Management, LLC and RELX Inc.

EXHIBIT B

US00RE48847E

(19) **United States**
(12) **Reissued Patent**
Isaacs

(10) **Patent Number: US RE48,847 E**
(45) **Date of Reissued Patent: Dec. 7, 2021**

(54) **POST-PAGE CALLER NAME IDENTIFICATION SYSTEM**

(71) Applicant: **Greenflight Venture Corporation**, West Palm Beach, FL (US)

(72) Inventor: **Jeffrey D. Isaacs**, Fort Washington, PA (US)

(21) Appl. No.: **15/289,905**

(22) Filed: **Oct. 10, 2016**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **8,861,698**
Issued: **Oct. 14, 2014**
Appl. No.: **14/174,724**
Filed: **Feb. 6, 2014**

(51) **Int. Cl.**
H04M 1/56 (2006.01)
H04M 15/06 (2006.01)
H04M 7/00 (2006.01)
H04M 3/42 (2006.01)

(52) **U.S. Cl.**
CPC ***H04M 7/0033*** (2013.01); ***H04M 3/42042*** (2013.01); *H04M 2201/38* (2013.01)

(58) **Field of Classification Search**
CPC H04M 3/42059; H04M 3/42042; H04M 7/0033; H04M 2201/38
USPC 379/142.1, 142.15
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,457,738 A * 10/1995 Sylvan 379/93.23
5,903,636 A * 5/1999 Malik H04M 3/42042 379/142.01
6,782,086 B2 * 8/2004 Clapper H04M 1/575 379/142.06
6,954,526 B1 * 10/2005 Glenn H04Q 3/0025 379/207.15
7,308,408 B1 * 12/2007 Stifelman G10L 15/22 704/266
7,839,987 B1 * 11/2010 Kirchhoff H04M 1/575 379/142.02
8,155,287 B2 * 4/2012 Woodring H04M 3/42 379/142.05
8,358,766 B1 * 1/2013 Denenberg H04M 3/42042 379/201.01
8,447,285 B1 * 5/2013 Bladon H04M 3/53341 455/414.4
8,625,762 B1 * 1/2014 White et al. 379/142.06
(Continued)

OTHER PUBLICATIONS

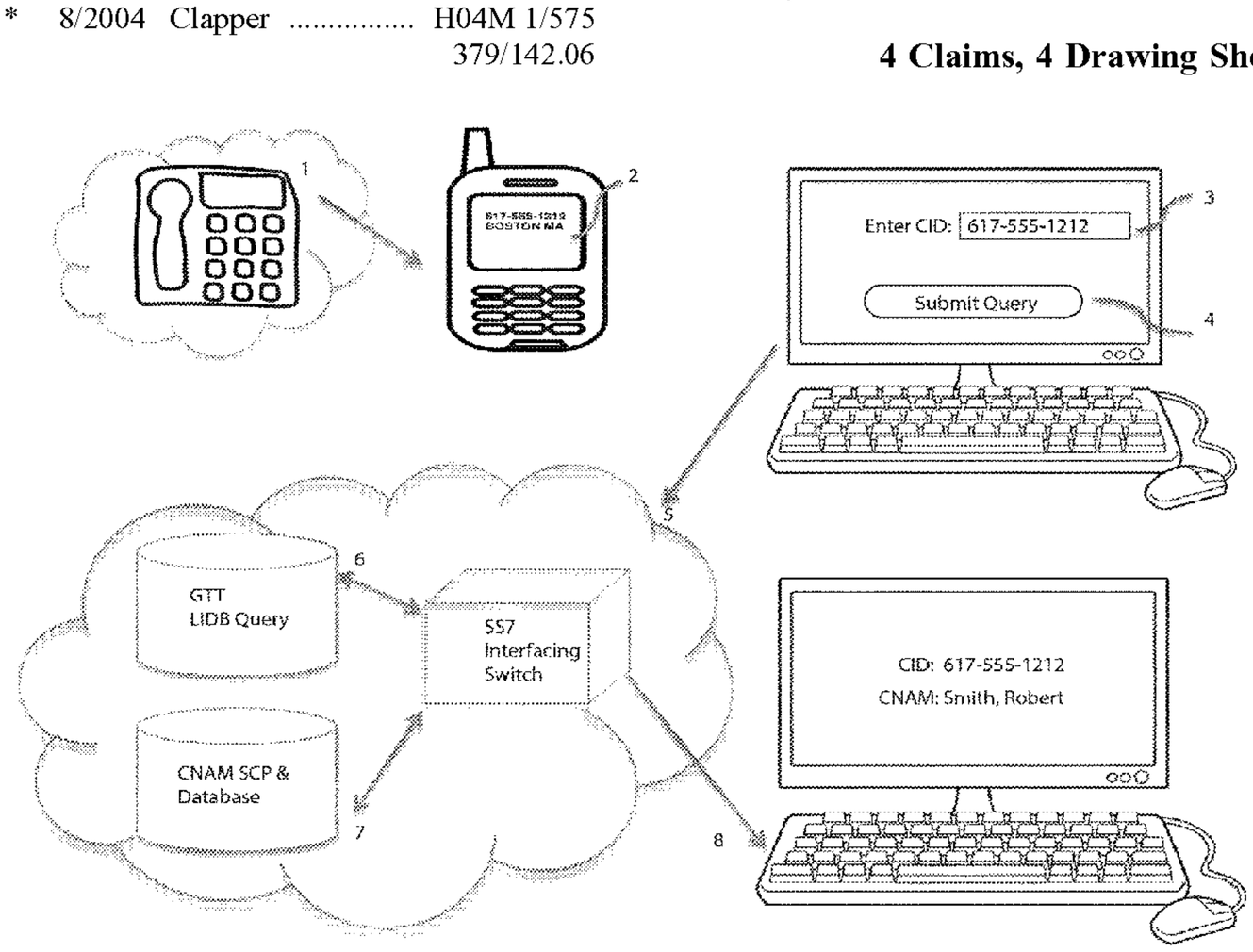
Kessler, "In Apps For Mobile Advertising, Brands Pay You To Listen" fastcompany.com, Sarah Kessler, Aug. 15, 2013, (pp. 1-10) (Hereinafter Kessler).*
3:16-cv-00175-RS *Greenflight Venture Corporation et al.* v. *Whitepages, Inc. et.*, "Order Granting Defendant's Motion for Judgment on the Pleadings," issued on Jul. 25, 2016.
(Continued)

Primary Examiner — Ovidio Escalante
(74) *Attorney, Agent, or Firm* — Edward C. Kwok; VLP Law Group, LLP

(57) **ABSTRACT**

Caller Name Identification, or CNAM Caller ID, is a telecommunication end-user feature that appeared for PSTN landline customers in the late 1980s. The rapid development of cellular mobile and VOIP telephony systems lead to the frequent omission of the CNAM Caller ID feature. Described is an independent end-user system that obtains the CNAM Caller ID after the call page transmission. The system operates on the user's smartphone or on a TCP/IP connected computer. A user with multiple telephone devices (i.e. a smartphone, landline, and VOIP line) may share use of this system between all devices.

4 Claims, 4 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

8,644,470	B2 *	2/2014	Gosselin	H04M 3/42042 379/142.06
8,699,682	B2 *	4/2014	Nguyen	H04Q 3/0016 379/114.03
9,641,663	B2 *	5/2017	Rincon	H04M 1/72561
2002/0099720	A1 *	7/2002	Bansal	707/104.1
2008/0037764	A1 *	2/2008	Lee	H04M 3/12 379/266.01
2008/0052372	A1 *	2/2008	Weber	G06F 16/58 709/217
2008/0147771	A1 *	6/2008	Bertolino	709/201
2008/0222144	A1 *	9/2008	Backer et al.	707/5
2008/0240383	A1 *	10/2008	Fronczak et al.	379/88.19
2009/0158367	A1 *	6/2009	Myers	H04N 21/25833 725/109
2009/0257575	A1 *	10/2009	Gosselin	H04M 3/42042 379/142.06
2009/0328118	A1 *	12/2009	Ravishankar et al.	725/106
2010/0254524	A1 *	10/2010	Kim	H04Q 3/76 379/201.02
2011/0013755	A1 *	1/2011	Martino	H04M 1/578 379/88.2
2011/0081911	A1 *	4/2011	Silver	H04M 5/12 455/445
2013/0287196	A1 *	10/2013	Zerillo	379/142.06

OTHER PUBLICATIONS

3:16-cv-00175-RS *Greenflight Venture Corporation et al.* v. *Whitepages, Inc. et.*, "Order Denying Applicant's Motion For Reconsideration," issued on Aug. 16, 2016.

Zhang, "The Line Information Database (LIDB) and Wireless Services," Telcordia Technologies, Inc., White Paper Analysis, Dec. 2001.

"OSSGR Section 22.3: Line Information Database," Telcordia, Apr. 2009, Issue 8 (GR-1158).

3:16-cv-00175-RS *Greenflight Venture Corporation et al.* v. *Whitepages, Inc. et.*, "Defendant Whitepages, Inc.'s Reply in Support of Its Motion for Judgment on the Pleadings of Invalidity under 35 USC 101," filed on Jun. 13, 2016.

3:16-cv-00175-RS *Greenflight Venture Corporation et al.* v. *Whitepages, Inc. et.*, "Whitepages, Inc.'s Opposition to Defendants' Motion for Reconsideration," filed on Aug. 9, 2016.

3:16-cv-00175-RS *Greenflight Venture Corporation et al.* v. *Whitepages, Inc. et.*, "Defendant Whitepages, Inc.'s Notice of Motion and Motion for Judgment on the Pleadings of Invalidity under 35 USC 101," filed on May 23, 2016.

3:16-cv-00175-RS *Greenflight Venture Corporation et al.* v. *Whitepages, Inc. et.*, "Defendants Greenflight Venture Corporation and Jeffrey Isaacs' Opposition to Motion for Judgment on the Pleadings of Invalidity under 35 USC 101," filed on Jun. 6, 2016.

3:16-cv-00175-RS *Greenflight Venture Corporation et al.* v. *Whitepages, Inc. et.*, "Defendants' Notice of Motion and Motion for Leave to File Motion for Reconsideration," filed on Jul. 29, 2016.

* cited by examiner

FIG. 1A -Prior Art-

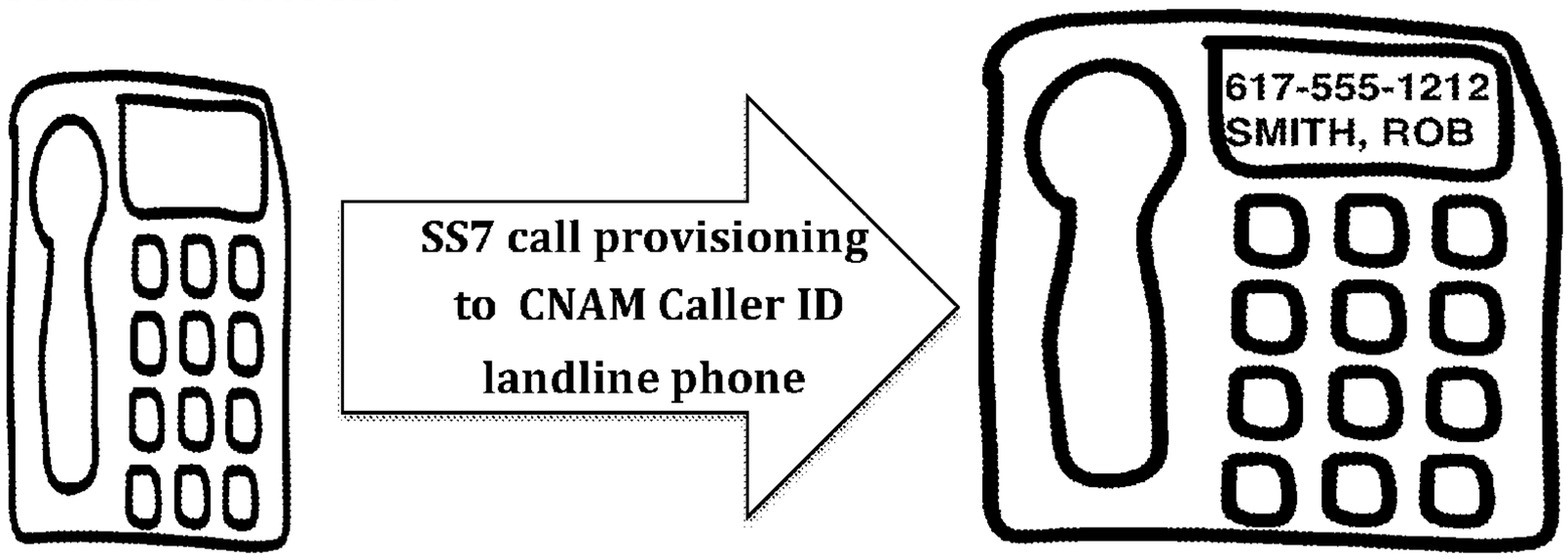


FIG. 1B -Prior Art-

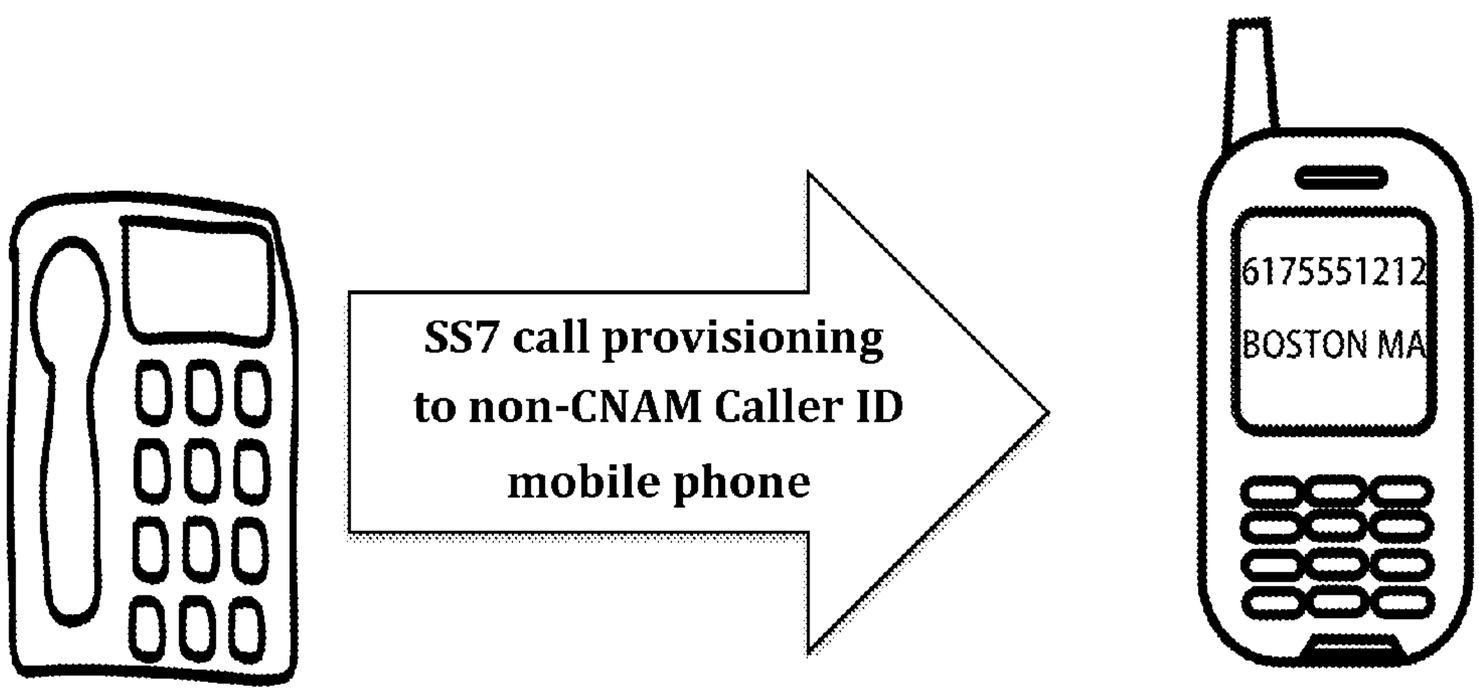
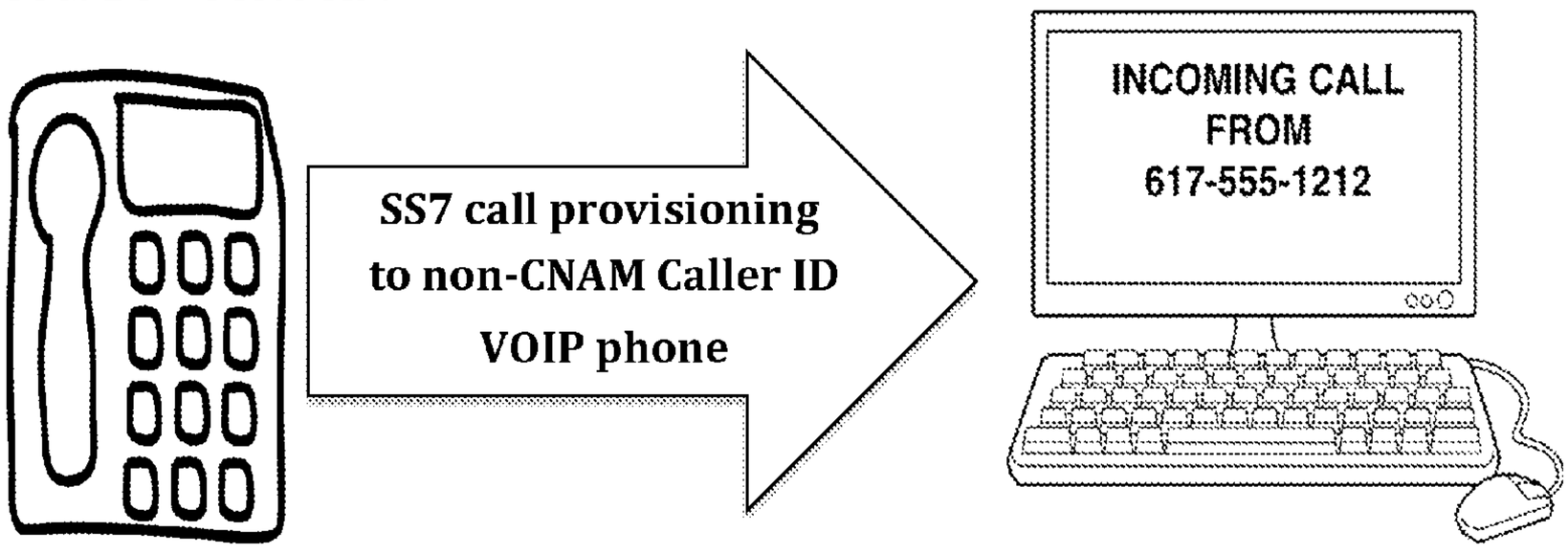


FIG. 1C -Prior Art-



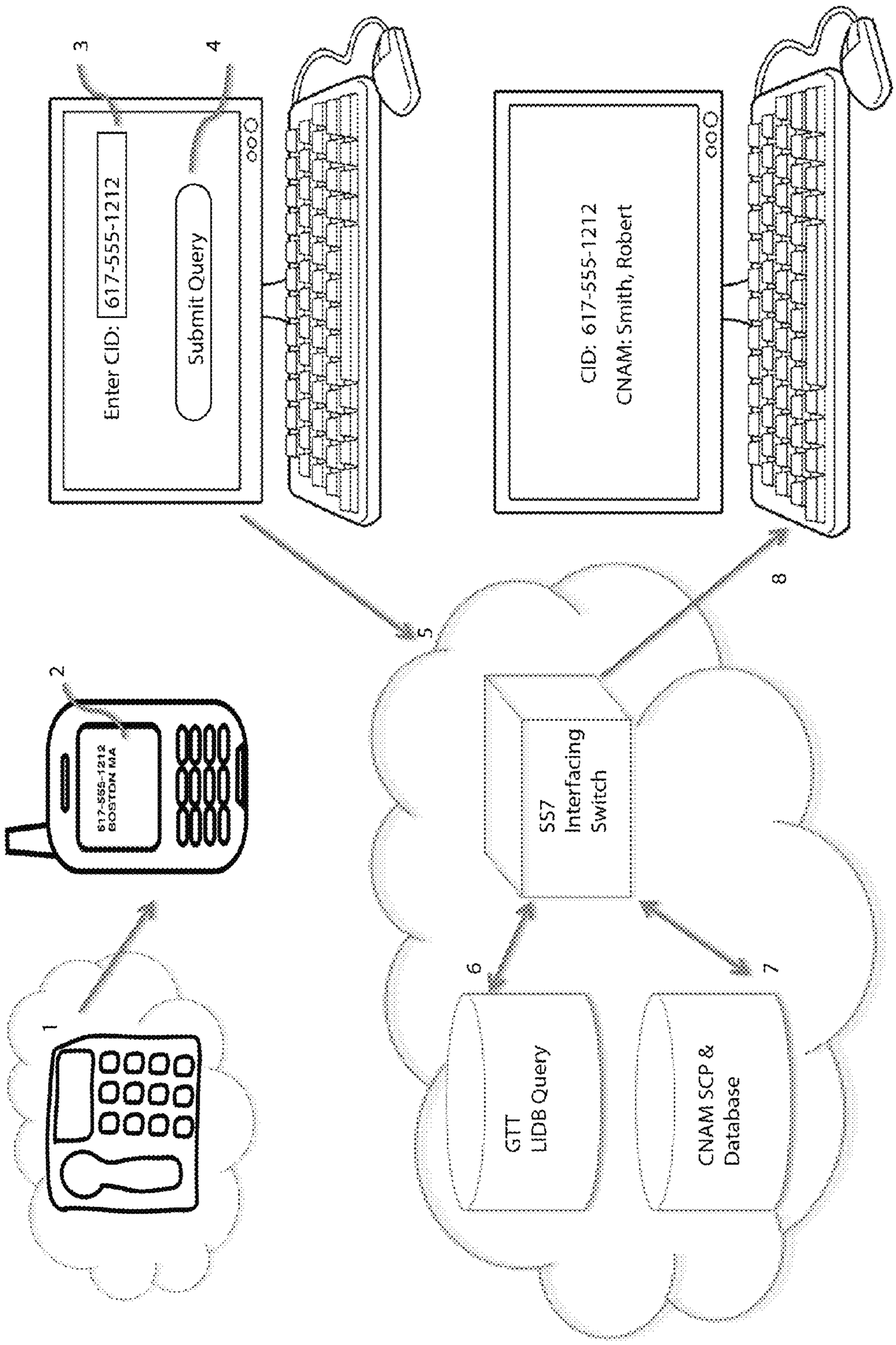
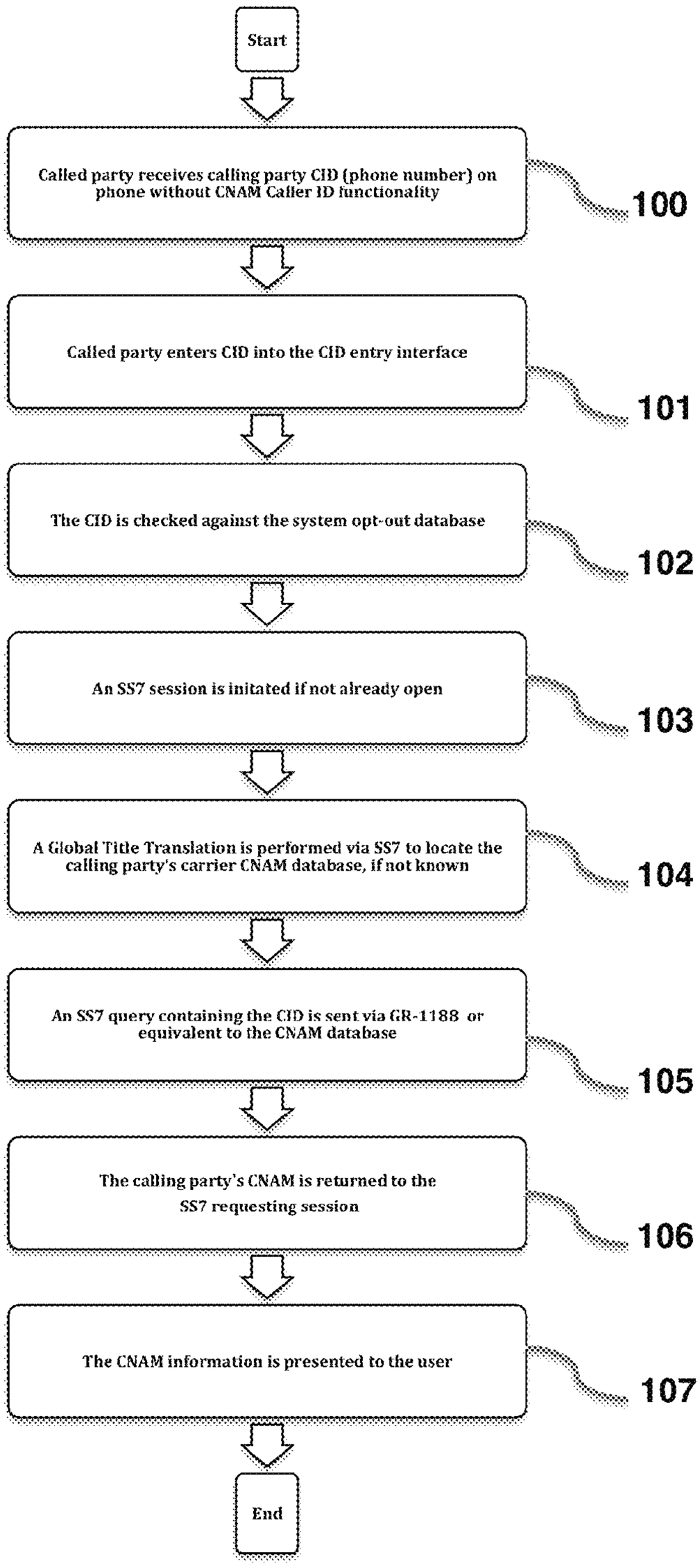

1
2
617-555-1212
BOSTON MA
3
Enter CID: 617-555-1212
4
Submit Query
5
6
GTT
LIDB Query
7
CNAM SCP &
Database
8
CID: 617-555-1212
CNAM: Smith, Robert
SS7
Interfacing
Switch

FIG. 2

FIG. 3


Start
Called party receives calling party CID (phone number) on phone without CNAM Caller ID functionality
100
Called party enters CID into the CID entry interface
101
The CID is checked against the system opt-out database
102
An SS7 session is initated if not already open
103
A Global Title Translation is performed via SS7 to locate the calling party's carrier CNAM database, if not known
104
An SS7 query containing the CID is sent via GR-1188 or equivalent to the CNAM database
105
The calling party's CNAM is returned to the SS7 requesting session
106
The CNAM information is presented to the user
107
End

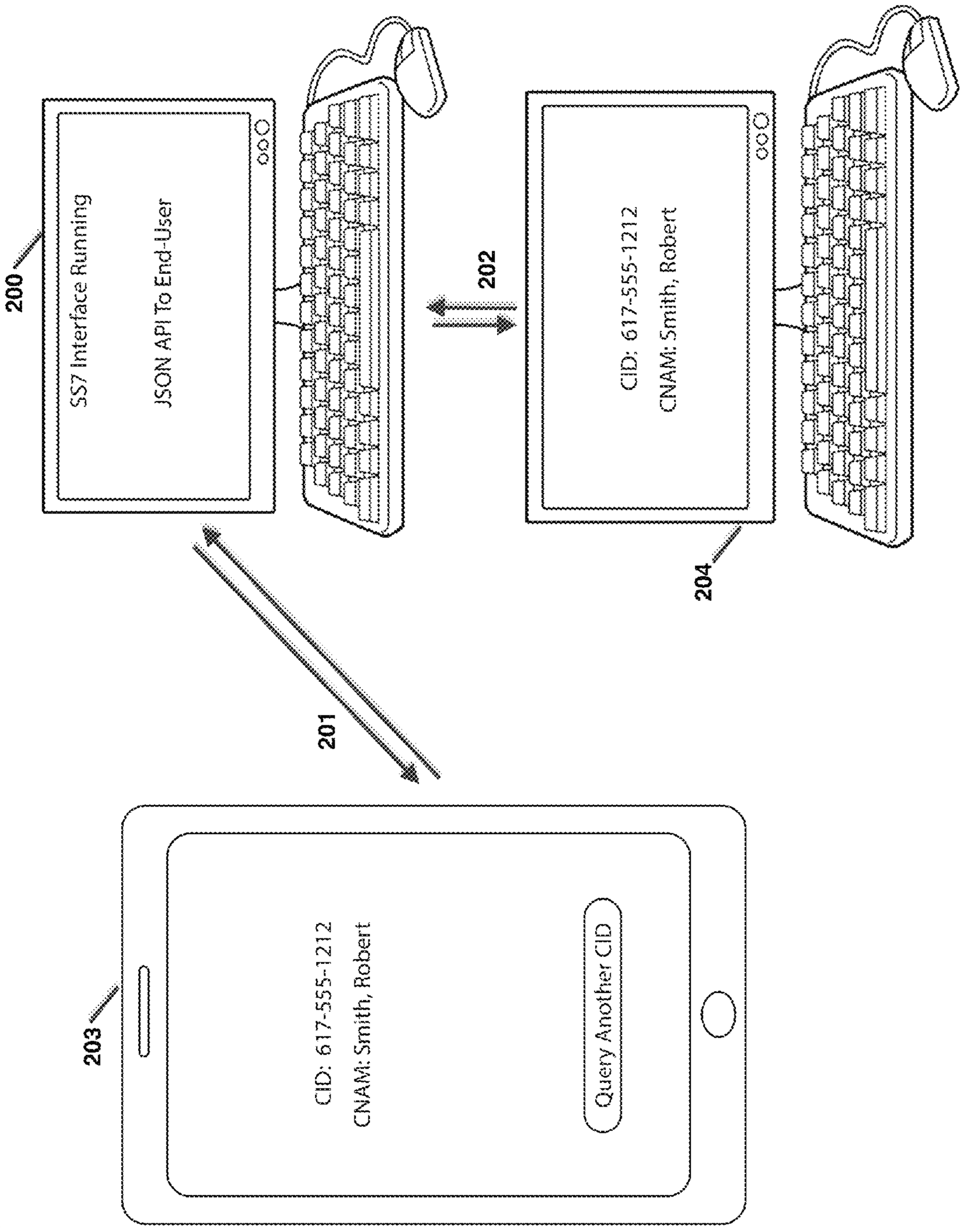

200
SS7 Interface Running
JSON API To End-User
201
202
CID: 617-555-1212
CNAM: Smith, Robert
204
203
CID: 617-555-1212
CNAM: Smith, Robert
Query Another CID

Fig. 4

POST-PAGE CALLER NAME IDENTIFICATION SYSTEM

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue; a claim printed with strikethrough indicates that the claim was canceled, disclaimed, or held invalid by a prior post-patent action or proceeding.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to caller identification systems. More specifically, it relates to a post-page caller name identification system that bridges SS7 retrievable caller data with a user-accessible IP interface. Carrier implementation of caller name identification has become increasingly complicated due to the fragmentation of service providers on the North American Public-Switched Telephone Network (PSTN). The present invention restores functionality of this important SS7/PSTN capability, caller name identification, to the increasing number of telecommunications end-users left without this feature.

2. Description of the Prior Art

To place a call using the earliest long-distance telephone systems, a calling party initiated a request with the local switchboard operator. The calling party's local operator would connect to the inward operator, and specify the called party. The inward operator would identify the calling party to the called party, then coordinate the completed telephone circuit with the originating local operator.

Direct dial systems using automated protocols over the Public Switched Telephone Network eventually phased out the operator switchboard system by the 1960's. Unlike the system utilizing human operators, the direct dial networks did not readily identify the calling party to the called party. The relative anonymity of automated PSTN systems created both inconvenience and the potential for abuse. The invention of what became known as caller identification addressed these shortfalls. Between 1969 and 1975, Mr. Theodore Paraskevakos successfully claimed twenty separate patents related to automatic telephone line identification. By 1989, Bell Atlantic, BellSouth, and U.S. West Communications had implemented caller identification in their consumer service offerings.

Caller identification, or Caller ID, may colloquially refer to the presentation of either the calling party's telephone number, or name, to the called party. The initial caller identification systems transmitted only the calling party's phone number to the called party. By their rollout in the late 1980's, or shortly thereafter, the "Baby Bell" Caller ID service offerings typically included both CID and CNAM functionality. These services grew in popularity, with tens of millions of subscribers by the late 1990's. For this specification, caller identification, or CID, refers to the presentation of the calling party's phone number to the called party. Caller name identification, or CNAM Caller ID, shall refer to the presentation of the calling party's name to the called party.

The technical protocols for Caller ID evolved since Mr. Paraskevakos' invention, to what is now industry-standard implementation over the PSTN SS7 network. Despite the standardization of the protocol, telephone line portability deregulation significantly increased the complexity and cost of a CNAM Caller ID query. CNAM information previously

held in a few databases of the Baby Bells increased to hundreds, if not thousands, of databases operated by the emerging telephone companies.

At the time of filing, a complete CID & CNAM Caller ID query typically involved the following steps: 1) the CID is transmitted from the calling party to the called party during SS7 call circuit provisioning (the network "page"), 2) a Global Title Translation (GTT) is initiated from the called party's SS7 signaling transfer point (STP) to determine which CNAM database and telephone carrier represents the calling party CID, 3) a GR-1188 CNAM query is relayed via SS7 to the service control point (SCP) for the respective CNAM database, and 4) the GR-1188 CNAM query result is presented to the called party. The exact sequence of events may vary depending upon the called and calling party's intercarrier agreements and SS7 implementation. Characteristic of the prior art implementations, the entire sequence of events takes place during the ringing or network page, and prior to the call completion.

As mobile phones and voice-over-IP telephony (VOIP) proliferated over the past decade, many providers never implemented full CNAM Caller ID to their mobile or VOIP end-users. Those that did implement CNAM Caller ID usually charge a monthly fee for CNAM Caller ID. For example, a major American wireless carrier recently began offering "Caller Name ID" as a premium monthly feature. Furthermore, individuals now may own several phone numbers, including a home land-line, a personal cellular mobile, and a VOIP line at work. Subscribing to a monthly CNAM service on multiple lines, if the feature is even available, is costly. As a result, CNAM Caller ID prevalence is trending backwards.

SUMMARY OF THE INVENTION

In view of the foregoing limitations inherent in the known types of caller identification systems present in the prior art, the present invention provides a post-page caller name identification system. This standalone system may function for multiple telephone devices owned or operated by the end-user. The system is independent of the end-user's carrier implementation (or lack thereof) of CNAM Caller ID.

The utility of the present invention, which shall be described subsequently in greater detail, is to identify the calling party's name when only the CID is known. This is typically the case with most modern cellular mobile and VOIP systems. The present invention's post-page functionality complements the prior art. In an ideal telephony network, CNAM Caller ID would be transmitted during the page, or ring. As described above, CNAM implementation has been declining for a decade due to increasing complexity of carriers. This necessitates the present invention as the next-best solution for an end-user wishing to identify a calling party.

To attain this, the present invention comprises a system that interfaces the user directly with the calling party's SS7 SCP-connected CNAM database. After a call or page terminates, the user accesses the present invention via the user terminal, which may operate on a mobile phone application or via direct HTML web access. The user inputs the CID information relayed from the calling party to the end-user. The system then performs a Global Title Translation (GTT) query using its SS7 node. The GTT lookup returns the respective phone carrier and CNAM database applicable to the CID. The system then performs a GR-1188 CNAM query via SS7 to the service control point (SCP) for the

respective CNAM database. Finally, the CNAM query result is presented on the user-interface.

By utilizing the present invention, the end-user consolidates CNAM services and enjoys significant cost savings. At time of filing, a commercial implementation of the present invention was offered free-of-charge to the user via either a smartphone applications or direct web access. As stated above, the CNAM functionality offered by the present invention is often unavailable, even as a premium service, on many VOIP and cellular carriers.

The calling party may opt-out from this process at three points. First, the calling party may opt-out from CID transmission on a per-call basis, which is typically known as "*67 Caller ID Block." Second, the calling party may inform his/her carrier to remove his information from their CNAM database. Third, the calling party may opt-out using a form implemented on the privacy policy page of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Features of the exemplary implementations of the invention will become apparent from the description, the claims, and the drawings in which:

FIG. **1** identified as subparts **1**A, **1**B, & **1**C, represents three typical variations of the caller identification prior art;

FIG. **2** is a graphical depiction of the core system components and their interactions;

FIG. **3** is a flow diagram enumerating each possible step the system performs to process a user query for caller name identification; and

FIG. **4** depicts two additional embodiments of the user interface.

DETAILED DESCRIPTION

From FIG. **1**, three scenarios are identified which represent the current prior art of caller identification systems. Scenario **1**A represents the ideal provisioning of a call where the called party receives both the name and phone number of the calling. In this case, the CID and CNAM are 617-555-1212 and "Smith, Robert," respectively. Scenario **1**B, the middle illustration, only provides the calling party phone number. This scenario is typical of most cellular mobile carriers. In lieu of the CNAM, the cellular carrier will approximate the location of the calling party, although this is frequently subject to error. Scenario **1**C, illustrated at the bottom of FIG. **1**, depicts a typical VOIP caller identification presentation, which only includes the calling party number (CID).

Having understood the possible combinations of CID and/or CNAM presentations possible on a caller identification system, FIG. **2** embodies the components of the present invention utilized in the context of the scenario depicted in FIG. **1**B. The calling party has placed a call (**1**) over the PSTN, and the carrier has provisioned for the CID and estimated location to be presented on the end-user's telephone screen (**2**) during the network page.

The end-user initiates use of the system by accessing the user terminal. The user enters the CID from (**2**) into the CID entry field (**3**) of the user terminal. After entering a valid CID, the user (**4**) submits the query to the system. The system then initiates the "CNAM database query" (**5**) via the SS7 network.

There exist several methodologies to obtain a CNAM database result via SS7, and the exact implementation depends upon the calling party's carrier, the system's carrier,

and any contractual relationships between the two carriers. Exemplified in FIG. **2**, and most typical, the system performs a Global Title Translation (**6**) using various Line Information Databases (LIDBs) to determine the calling party's carrier. In some cases, the system will already know the calling party's carrier (e.g. if they are the same as the called party), and this step will be unnecessary. Once the carrier is known, the system is able to route a CNAM query using GR-1188 (**7**) to the appropriate SS7 signal control point (SCP). The SCP controls CNAM database access for a given phone carrier. For the purposes of this invention, the entire process is referred to as "CNAM Database Query" (**5**) and refers to any of the proper SS7 methods to retrieve CNAM information.

Upon successful CNAM database query, the CNAM Caller ID is relayed back to the user terminal. The caller name identification is displayed on the appropriate user interface element, thereby completing the process.

FIG. **3** serves as a flow diagram enumerating all possible steps for the system, as embodied, to carry out its function. The utilization of this system commences upon end-user receipt of a CID page (**100**). The user then activates the system by entering the page CID into the CID entry interface (**101**). Before the system proceeds, it first validates that the CID is not listed within the system's opt-out privacy database (**102**). At this stage, the system may also ask the user to confirm the CID had been transmitted to a telephone device they own or operate.

The system then instructs the SS7 interfacing node to initiate an SS7 session, if one is not already active (**103**). The exact state or instructions relayed to the SS7 switch/node varies depending upon carrier implementation. Once the SS7 session is active, a Global Title Translation (GTT) is performed using the CID from the CID entry interface. (**104**). The GTT returns the calling party carrier information necessary to locate the carrier's CNAM database on the SS7 network. A query is thereafter sent, usually via the GR-1188 protocol, to the signal control point (SCP) for the calling carrier CNAM database (**105**). Assuming the calling party didn't opt-out from its carrier CNAM database, the calling party's CNAM is returned to the system's SS7 node (**106**). Then, the CNAM database query result is displayed on the user interface (**107**).

FIG. **4** depicts additional embodiments of the system relating to its user interface. In this illustration, the system's SS7 interface (**200**) is physically separated from its user interface. The user interface is implemented on either another computer linked via the TCP/IP (**204**), or the end-user's telephone that received the initial call page (**203**). The SS7 interface communicates (**201** or **202**) with the user interface via an industry standard API protocol such as JSON.

I claim:

[1. A system, functioning independently of a called party's telephone carrier and device, provides a calling party's CNAM after entry of the calling party's telephone number CID, comprising:

a) an entry field, within a HTML web or mobile phone application, permitting the called party to input a query, post-page, specifying the CID;

b) an SS7 interfacing node permitting real-time access to the SS7 network;

c) a function serving as a direct interface between the called party's query and the calling party carrier's respective CNAM database;

d) within the HTML web or mobile phone application, a display of the successfully queried calling party CNAM.]

[2. The system of claim 1, wherein the web or mobile phone application provides free-of-charge CNAM resolution for any of the end-user's multiple telephony devices, thereby permitting cost-savings.]

[3. The system of claim 1, wherein the called party enjoys significant cost savings and free-of-charge CNAM querying through an advertising display within the user interface.]

[4. The system of claim 1, wherein component function (c) additionally:

confirms that the CID is not subject to system opt-out privacy controls; and

confirms that the CID paged a telephonic device owned or operated by the called party.]

[5. A method for providing a called party with the calling party's CNAM after a network page, independent of interaction with the carrier or device receiving the page, comprising the following steps:

a) entering of the calling party's telephone number CID into a web HTML or mobile phone application query field;

b) connecting to the PSTN via an SS7 interfacing node;

c) directly querying the calling party carrier CNAM database with the CID query entry;

d) displaying the successfully queried calling party CNAM on the HTML web or mobile phone application user interface.]

[6. The method of claim 5, further comprising a step to display advertising sponsorship on the web or mobile phone application interface, thereby achieving significant user cost savings and free-of-charge CNAM querying.]

7. An SS7 interfacing node connected to both a TCP/IP network and an SS7 communication network, comprising:

a TCP/IP network interface configured to provide a connection to a user terminal, the connection being configurable over an application program interface (API) using an industry standard protocol; and

an SS7 communication network interface configured to communicate with signal control points (SCPs) on the SS7 communication network;

wherein the SS7 interfacing node is configured (a) to receive from the user terminal over the TCP/IP network interface a query of a caller name identification (CNAM) database for a CNAM based on a telephone number obtained from a paging signal of an SS7 call,

(b) to transmit the telephone number in a carrier identity request over the SS7 communication network interface to one or more line information databases (LIDBs); (c) to receive a carrier identity from the LIDBs over the SS7 communication network interface; (d) based on the carrier identity, to forward the query using GR-1188 to one or more CNAM databases over the SS7 communication network interface, (e) over the SS7 communication network interface, to receive from the CNAM databases a CNAM associated with the telephone number; and (f) over the TCP/IP network interface, to provide the received CNAM as the calling party's name to the user terminal.

8. The SS7 interfacing node of claim 7, wherein the industry standard protocol comprises JSON.

9. A method in an SS7 interfacing node connected to both a TCP/IP network and an SS7 telecommunication network, comprising:

configuring a TCP/IP network interface with a user terminal using an application program interface (API) that conforms to an industry standard protocol; and

configuring an SS7 communication network interface that communicates with one or more line information databases (LIDBs) and one or more SS7 signal control points (SCPs) over the SS7 communication network;

wherein the SS7 interfacing node (a) receives from the user terminal over the TCP/IP network interface a query of a caller name identification (CNAM) database for a CNAM based on a telephone number obtained from a paging signal of an SS7 call, (b) transmits the telephone number in a carrier identity request over the SS7 communication network interface to one or more line information databases (LIDBs); (c) receives a carrier identity from the LIDBs over the SS7 communication network interface; (d) based on the carrier identity, forwards the query using GR-1188 to one or more CNAM databases over the SS7 communication network interface, (e) over the SS7 communication network interface, receives from the CNAM databases a CNAM associated with the telephone number; and (f) over the TCP/IP network interface, provides the received CNAM as the calling party's name to the user terminal.

10. The method of claim 9, wherein the industry standard protocol comprises JSON.

* * * * *